

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
COLUMBIA DIVISION**

KASSANDRE CLAYTON, KATHLEEN  
ARMAN, SONYA GARCIA-MARTINEZ,  
JOSEPH FRONTERA, ANGELA MAHER,  
RALPH PERAGRINE, MICHELE  
PETTIFORD, THERESA WELSH, LATRICIA  
FORD, CLIFFORD SCOTT, ROBERT  
WATTS, JR., JASON MONEY, NICOLE  
MONEY, individually and on behalf of all  
others similarly situated,

Plaintiffs,

v.

BLACKBAUD, INC.,

Defendant.

Case No. 3:21-01058-JMC

MDL No. 2972

**CLASS ACTION COMPLAINT**

Plaintiffs Kassandre Clayton, Kathleen Arman, Sonya Garcia-Martinez, Joseph Frontera, Angela Maher, Ralph Peragrine, Michele Pettiford, Theresa Welsh, Latricia Ford, Clifford Scott, Robert Watts, Jr., Jason Money, and Nicole Money, individually and on behalf of all others similarly situated (“Plaintiffs”), bring this action against Defendant Blackbaud, Inc. (“Blackbaud”), seeking monetary damages, restitution, and/or injunctive relief. Plaintiffs make the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation of their counsel and facts that are a matter of public record.

## **I. INTRODUCTION**

1. This lawsuit exists because cybercriminals unsurprisingly targeted a company in the business of storing personal information, demanding payment to supposedly delete the data that they stole. Such a payment, or a “ransom,” is paid by companies who acquiesce to data publication extortion demands when they are trying to prevent the public, victims, and shareholders from learning about a data breach.<sup>1</sup> After data was stolen from its servers, Blackbaud paid a ransom for the cybercriminals’ assurances that stolen data was “deleted.” But the breach became public anyway. Now, Blackbaud is trying to spin its extortion payment as its way of having successfully “stopped” a ransomware attack, despite the fact that cybercriminals had already stolen the very data Blackbaud was entrusted to protect.

2. Blackbaud is a successful data security company, having created a niche market in—and profiting handsomely from—data security for some of the most highly-sensitive information that exists: personal information from donors, patients, students, and congregants.

---

<sup>1</sup> Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), <https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/>.

3. The value of this information is recognized by several, different constituencies. First, the value is recognized by Blackbaud, which can attribute its business model to the existence of this information, and the need to keep it safe. Second, the value is recognized by cybercriminals, who know that this type of data can be exploited for ransom payments and to commit identity theft. And third, the value is recognized by the individuals, themselves, whose data was stolen.

4. Blackbaud identifies itself as the “world’s leading cloud software company powering social good,” a job on which it claims to have been “100% focused” “[s]ince day one.”<sup>2</sup> Blackbaud markets its expertise in safeguarding information to those organizations who normally do not have access to high-level information security (such as art and cultural organizations, companies, faith communities, foundations, healthcare organizations, higher education institutions, individual change agents, K-12 schools, and nonprofit organizations)—not only because statutory schemes require certain levels of data security, but to thwart cybersecurity attacks. These vulnerable “Social Good Entities,” as described below, rely on Blackbaud to deliver the strong security practices it promises, because their donors, students, patients, and congregants count on the security of their data in order to engage with these organizations.

5. Millions of individuals have shared their most valuable data with Social Good Entities based on the ordinary, reasonable understanding that their information would be handled and maintained with appropriate safety standards—the very services that Blackbaud was engaged to and promised to perform.

6. Despite Blackbaud’s representations that it provided robust cybersecurity services, in reality, its security program was woefully inadequate. Blackbaud’s unsound, vulnerable systems containing valuable data were an open invitation for a months-long intrusion and exfiltration by

---

<sup>2</sup> Blackbaud, Inc., <https://www.blackbaud.com/> (last visited Mar. 30, 2020).

cybercriminals, who were seeking to exploit the valuable nature of the information to extract a ransom from Blackbaud, among other unlawful activities.

7. Rather than disclose the theft and initiate protections for the victims, Blackbaud remained silent for months while secretly attempting to buy off the criminals who had stolen and then held this valuable data hostage, paying a handsome ransom. Apparently relying only on the concept of “honor among thieves,” Blackbaud claims that the cybercriminals who breached its systems, stole the valuable and sensitive data, and held it ransom, were trustworthy and could be counted on for the level of responsibility, fidelity, and security for private data that Blackbaud itself failed to show.

8. Despite guidance from the federal government, regulatory bodies, and cybersecurity professionals warning companies not to pay ransoms to cybercriminals, Blackbaud negotiated payment, and now asserts that it “discovered and stopped a ransomware attack.”<sup>3</sup> But Blackbaud’s payment has only demonstrated that it was willing to make at least one payment to prevent the data from being disclosed—a powerful message to individuals with access to the very information that facilitates identity theft and health insurance fraud.

9. Instead of providing fulsome notice to the individuals who were impacted by the ransomware attack, Blackbaud has downplayed the incident, insisting that, although cybercriminals were able to exfiltrate information from Blackbaud’s system, those same criminals can be trusted to have destroyed any copies of the data. As a result, Plaintiffs and class members are left with empty platitudes instead of vital information that would allow them to take proactive measures to prevent identity theft and future fraud.

---

<sup>3</sup> Blackbaud, *Learn more about the ransomware attack we recently stopped* (July 16, 2020), <https://www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped>.

10. Blackbaud’s unlawfully deficient data security and utter failure, even now, to honestly address the breach has injured millions of donors, students, and patients, the Plaintiffs and putative class members in this action.

## **II. NATURE OF THE ACTION**

11. Blackbaud describes itself as “the world’s leading cloud software company powering social good[,]” and claims it “equip[s] change agents with cloud software, services, expertise, and data intelligence designed with unmatched insight and supported with unparalleled commitment.”<sup>4</sup> According to Blackbaud, “[e]very day, [its] customers achieve unmatched impact as they advance their missions.”<sup>5</sup> Furthermore, as it repeatedly represented in investor presentations, “[s]ocial good is a significant global sector.”<sup>6</sup> According to its website, its clients include arts and cultural organizations, companies (conducting corporate social responsibility activities), faith communities, foundations, healthcare organizations, higher education institutions, individual change agents, K-12 schools, and nonprofit organizations (the “Social Good Entities”).<sup>7</sup> Plaintiffs and class members are the Social Good Entities’ donors, students, patients, and congregants.

12. Blackbaud touts the success of its business: “Blackbaud has grown to serve millions of users across more than 100 countries, including one out of three Fortune 500 companies, 80% of the most influential nonprofits, 30 of the 32 largest nonprofit hospitals, 93% of higher education

---

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> *See, e.g.*, Investor Presentations dated July 30, 2019, October 16, 2019, May 5, 2020, July 29, 2020, October 28, 2020, and February 8, 2021.

<sup>7</sup> *Who We Serve & Industries We Support*, Blackbaud, <https://www.blackbaud.com/who-we-serve> (last visited Mar. 15, 2021).

institutions with billion-dollar campaigns, 25 of the largest Catholic Dioceses in the US and more.”<sup>8</sup>

13. Blackbaud has created a profitable business by catering to the needs of Social Good Entities—namely, providing data security services for information that it knows is incredibly valuable. According to Blackbaud’s most recent Form 10-K filed with the Securities and Exchange Commission (“SEC”) on February 23, 2021 (the “2020 Form 10-K”):

Many social good organizations use manual methods or software applications not specifically designed for fundraising and organizational management for institutions like theirs. Such methods are often costly and inefficient because of the difficulties in effectively collecting, sharing and using donation-related information. Furthermore, general purpose software applications frequently have limited functionality for the unique needs of our customer base and do not efficiently integrate multiple databases . . . .

\* \* \* \* \*

Because of these challenges, [Blackbaud] believe[s] nonprofits, education institutions, healthcare organizations and houses of worship can benefit from software applications and services specifically designed to serve their particular needs and workflows to grow revenue, work effectively and accomplish their missions.

14. Blackbaud markets itself to Social Good Entities by developing data-hosting “solutions” to meet those entities’ needs; Blackbaud knows that nonprofits devote their resources to fundraising and benefit management and are unable to benefit from the economy of scale afforded by large scale data warehousing and management. Requisite security for such information requires management by a third party specializing in competent management of data, compliant with the representations made to donors, and other obligations by contract, regulation, and statute. As part of its solutions-based services, Blackbaud assured its customers, prior to the discovery of

---

<sup>8</sup> Blackbaud, *Blackbaud CEO Mike Giononi Named One of 50 Most Influential by Charleston Business Magazine* (Mar. 12, 2021), <https://totalcampus.blackbaud.com/newsroom/article/2021/03/12/blackbaud-ceo-mike-gianoni-named-one-of-50-most-influential-by-charleston-business-magazine>.

the Data Breach (described further below), that Blackbaud employed “world-class security, privacy, and risk management teams” to ensure the safety of data entrusted to Blackbaud.<sup>9</sup> Blackbaud assured its customers, who entrusted Plaintiffs’ and class members’ data to Blackbaud, that it had robust cybersecurity practices in place, which are known in the industry as specifically designed to thwart cybercrime like the Data Breach that took place here.<sup>10</sup>

15. Blackbaud knew that the information it hosted from the Social Good Entities contained some of class members’ most valuable personal information. Like other entities that host such information, Blackbaud knew that hosting such information made it an attractive target for cybercrime, noting that it “may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data[.]”<sup>11</sup>

16. Sophisticated companies like Blackbaud are aware of the different types of threat actors acting across the Internet and the type of security exploits they employ for profit. Accordingly, it is imperative that, as a company that specializes in and profits off of providing data security services to others, it guards against those exploits.

---

<sup>9</sup> Blackbaud Security (Mar. 2, 2020), <https://web.archive.org/web/20200302212750/https://www.blackbaud.com/security>. Throughout this Complaint, Plaintiffs cite to previously-imaged versions of Blackbaud’s website. Those images are housed by an independent, third party called the “WayBack Machine.” Courts have previously taken judicial notice of web pages available through the WayBack Machine. *See, e.g., Pohl v. MH Sub I, LLC*, 332 F.R.D. 713, 716 (N.D. Fla. 2019) (collecting cases). Plaintiffs have no reason to doubt the authenticity of the WayBack Machine’s archive of Blackbaud’s website and will obtain evidence confirming its accuracy as the case progresses.

<sup>10</sup> *Id.*

<sup>11</sup> *See, e.g.*, Form 10-K filed with the SEC on February 24, 2016, February 22, 2017, February 20, 2018, February 20, 2019, February 20, 2020, and February 23, 2021.

17. One typical type of exploit is called a “ransomware attack,” where an entity uses malicious code to encrypt data on a local machine, demanding a ransom for an encryption key to allow an entity to access the encrypted files again.<sup>12</sup>

18. A far more nefarious and dangerous exploit is when a criminal enterprise is able to exfiltrate data from an entity’s systems and demand a payment for that data’s return. Although some describe this type of attack as a “ransomware attack,” as well, the damage is far greater than a typical ransomware attack because the criminal enterprise is in possession of the information, and payment of the demanded ransom (or blackmail) cannot guarantee its destruction.

19. On July 16, 2020, a breaking news story by The NonProfit Times reported that Blackbaud had been the subject of a ransomware attack and data breach (the “Data Breach”). Blackbaud claimed it first learned of the Data Breach in May 2020.<sup>13</sup> According to the article, Blackbaud made a demanded blackmail payment to a cybercriminal in an undisclosed amount using Bitcoin.<sup>14</sup> The victims of the Data Breach were Plaintiffs and class members. As reported by The NonProfit Times, a Blackbaud spokesperson sought to assure consumers that “[c]redit card information, bank account information, or Social Security numbers were not stolen” and that Blackbaud claimed it had “credible information” that the data that was stolen went no further than the cybercriminals.<sup>15</sup> On that same day, Blackbaud also issued a statement regarding the Data

---

<sup>12</sup> Federal Bureau of Investigation, Scams and Safety, Common Scams and Crimes, *Ransomware*, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware> (last visited Mar. 27, 2021).

<sup>13</sup> Paul Clolery, *Breaking: Blackbaud Hacked, Ransom Paid*, NonProfit Times (July 16, 2020), [https://www.thenonproffitimes.com/npt\\_articles/breaking-blackbaud-hacked-ransom-paid](https://www.thenonproffitimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid).

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*



Breach on its website.<sup>16</sup> Despite this, in its 2020 Form 10-K, Blackbaud touted that: “[i]n 2020, [it] showed why [Blackbaud] continue[s] to be the trusted leader in this space.”<sup>17</sup> The information that Blackbaud disseminated regarding the Data Breach was misleading and inaccurate in numerous material ways.

20. The release, disclosure, and publication of a person’s sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.<sup>18</sup> A data breach can have grave consequences for victims for many years after the actual date of the breach—with the obtained information, identity thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, or obtain driver’s licenses in the victims’ names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

21. When information is stolen by cybercriminals, the risk of identity theft does not go away simply because an entity elects to submit to the cybercriminals’ demand for a ransom or blackmail payment. If anything, payment of a ransom demonstrates to cybercriminals that the data has value and can continue to be exploited for future payments—not just by the entity from whom the data was stolen, but from the individuals whose data was stolen, themselves.

22. Blackbaud was keenly aware of the risks of cyberattacks and breaches of its customers’ confidential data. It knew of the risk because Blackbaud had already suffered a

---

<sup>16</sup> *Learn More About the Ransomware Attack We Recently Stopped*, Blackbaud (July 16, 2020, 1:30 PM), <https://www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped>.

<sup>17</sup> Blackbaud 2020 Form 10-K.

<sup>18</sup> Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, S.C. Law (May 2014).

cybersecurity incident in which the laptop belonging to a Blackbaud employee was stolen from the employee's vehicle, after the employee had copied Private Information from donors onto the device.<sup>19</sup> At the time the breach was reported, Blackbaud insisted that it would “move immediately to do everything we can to help our customers and notify the people whose names and personal information are on those files.”<sup>20</sup> It took nearly eight months to disclose that the breach also impacted 84,000 University of North Dakota donors.<sup>21</sup>

23. Blackbaud also showed that it knew of the risk it faced by virtue of its own representations. In its Annual Report filed with the SEC, Blackbaud noted that the “secure collection, storage, and transmission of confidential” data is fundamental to its business.<sup>22</sup> Blackbaud likewise was aware of the significant risk of cyberattacks, identifying security breaches and theft of confidential donor data as a vulnerability.<sup>23</sup> In that same document, Blackbaud also acknowledged its obligation of notification in the event of a breach.<sup>24</sup>

24. Nevertheless, in February 2020—the same month Blackbaud acknowledged this risk—Blackbaud failed to stop the Data Breach. Blackbaud failed to detect the initial ransomware attack, and for three and a half months, between February 7, 2020, and May 20, 2020, cybercriminals orchestrated what Blackbaud has downplayed as a “security incident,” in which

---

<sup>19</sup> Identity Theft Resource Center 2008 Breach List (Jan. 2, 2009), [https://www.idtheftcenter.org/images/breach/Breach\\_Report\\_2008.pdf](https://www.idtheftcenter.org/images/breach/Breach_Report_2008.pdf).

<sup>20</sup> Nicole McGougan, Blackbaud: Press Release (Oct. 25, 2008), <https://www.blackbaud.com/newsroom/article/2008/10/25/blackbaud-press-release>.

<sup>21</sup> (Update) ND: Stolen laptop contained donors' financial data, DataBreaches.net (June 17, 2009), <https://www.databreaches.net/update-nd-stolen-laptop-contained-donors-financial-data/>.

<sup>22</sup> Blackbaud, Inc., Annual Report (Form 10-K) (hereinafter “2019 Form 10-K”) at 20 (Feb. 20, 2020), <https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417>.

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

they exploited Blackbaud's inadequately-protected computer networks, gained access to data, and copied data and servers managed, maintained, and secured by Blackbaud.<sup>25</sup>

25. Although Blackbaud initially represented to the public, law enforcement, and the Social Good Entities that sensitive information such as Social Security numbers ("SSN") and bank account numbers were not compromised, in a Form 8-K filing with the SEC on September 29, 2020, Blackbaud buried in its disclosures that this information was actually stolen during the "security incident."<sup>26</sup> This was the first time that Blackbaud publicly acknowledged that the information taken in the Data Breach included not only names and addresses, but also that "further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords."<sup>27</sup>

26. Blackbaud's servers contained Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information" or "PI") of individuals, including Plaintiffs. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."<sup>28</sup> PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§

---

<sup>25</sup> Blackbaud, Inc., Form 8-K at 2 (Sept. 29, 2020), <https://investor.blackbaud.com/static-files/58a4ae64-afc5-45f7-81df-69dfc93888fc>. This attack was not a typical "ransomware" attack; the cybercriminals did not encrypt Blackbaud's environment with malware to extort payment for decryption, as is standard in most ransomware attacks, but rather exfiltrated a copy of data from Blackbaud's environment and issued a ransom on the exfiltrated data. *See supra* n.3.

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), [https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress\\_enforcement\\_database\\_red\\_privacy\\_impact\\_assessment\\_june\\_2019.pdf](https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf).

1320d, et seq., as well as multiple state statutes. According to the U.S. Department of Health & Human Services (“HHS”), PHI “is information, including demographic data,” that relates to: “the individual’s past, present or future physical or mental health or condition,” “the provision of health care to the individual,” or “the past, present, or future payment for the provision of health care to the individual,” and that “identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.” Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, SSN).”<sup>29</sup>

27. According to Confidential Witness No. 1, a former information security analyst at Blackbaud, Blackbaud failed to maintain its information on current databases—it failed to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

28. According to Confidential Witness No. 1, his team suggested a year prior to the Data Breach that the data on Blackbaud’s servers needed to be encrypted to reduce vulnerabilities; however, because the servers were so old, the “exact nature of the data was unknown.”

29. While most information about the Data Breach remains fuzzy given Blackbaud’s failure to disclose the full details of its investigation of the breach to the public—including how many entities were impacted by the beach—the sources of the information largely fall into three categories:

---

<sup>29</sup> See HHS, Summary of the HIPAA Privacy Rule, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Mar. 24, 2021).

Healthcare Information	Educational Information	Information from Nonprofits and NGOs
Healthcare organizations across the globe use Blackbaud as their cloud software company. Most of the information impacted appears to be donor information; however, a significant number of notices have been sent to patients concerning exposure of PHI.	Blackbaud offers management software to K-12 schools, as well as universities. Some of the management software includes student information, learning management, enrollment management, and school websites. Most of the information impacted appears to be donor information, alumni information, student I.D. numbers, and student demographic information.	Nonprofits appear to be the largest users of Blackbaud's services. Blackbaud offers an array of software services that cater to nonprofits worldwide, but is best known for its customer relationship management ("CRM") tools. Many nonprofits use CRMs to nurture donors and fundraise.

30. As a result of this Data Breach, Plaintiffs and millions of class members have suffered and will continue to suffer concrete and actual harm.<sup>30</sup> Plaintiffs' and the class members' sensitive Private Information—which was entrusted to Blackbaud over the course of several years through the Social Good Entities, including educational institutions, hospital and healthcare systems, religious organizations, and charitable institutions—was compromised and unlawfully accessed as a result of the Data Breach and made subject to unlawful use by cybercriminals.

31. The cybercriminals who committed the Data Breach understand that the stolen data has value—Blackbaud has already paid a ransom to ensure its alleged destruction. But criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments (from either Blackbaud or the individual consumers affected), or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers

---

<sup>30</sup> Jessica Davis, *Blackbaud Confirms Hackers Stole Some SSNs, As Lawsuits Increase*, HealthITSecurity (Sept. 30, 2020), <https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase>.

also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.<sup>31</sup>

32. Blackbaud continues to tout the fact that it acquiesced to the cybercriminals' extortion demands as a success, noting that the payment "prevented the cybercriminal from blocking our system access and fully encrypting files," and somehow guaranteed that information that was stolen from Blackbaud's servers had been deleted.<sup>32</sup> Accordingly, and against professional guidance from cybersecurity professionals to the contrary, Blackbaud assumes that it has "no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly."<sup>33</sup>

33. According to Confidential Witness No. 1, it would be very difficult for Blackbaud to determine if the cybercriminals involved in this case would agree not to release the stolen Private Information publicly, despite payment of a ransom. "There is no good way to verify that," Confidential Witness No. 1 says. Further, Confidential Witness No. 1 says that s/he is "bothered" by Blackbaud's public statement that the cybercriminals destroyed the stolen data. S/he further stated, "[The cybercriminal] is a criminal. You don't trust him."

34. Blackbaud refuses to provide detailed information, leaving consumers to fill in the blanks. They are forced to simply rely upon notices of the Data Breach from entities that contracted with Blackbaud to host the data ("Notices"), which are just as confused. As a result, and because Blackbaud has refused to provide consumers with basic information that they could use to protect

---

<sup>31</sup> Krebs, *Why Paying to Delete Stolen Data is Bonkers*, *supra* n.1.

<sup>32</sup> *Learn More About the Ransomware Attack We Recently Stopped*, *supra* n.3.

<sup>33</sup> *Id.*

themselves and take specific, preventative measures, Plaintiffs and class members incurred out-of-pocket costs, including the cost of identity theft protection and insurance services, as well as time spent on taking preventative measures and responding to actual incidents of identity theft and fraud.

35. Despite knowing the devastating reach of the Data Breach, Blackbaud continues to misrepresent the extent of the breach on its website.<sup>34</sup> Contrary to Blackbaud's continued representations, as reflected in its statement related to the Data Breach and the Notices that Plaintiffs received, credit card numbers, bank account numbers, and/or other Private Information were compromised.

36. Despite Blackbaud's prior representations to the contrary, the public is now able to cobble together that that information compromised in the Data Breach included at least the following categories of Private Information:

- a. Personal identifiers, including full name, title, age, date of birth, and SSNs;
- b. Contact information, including addresses, phone numbers, email addresses, and LinkedIn profiles;
- c. Financial information, including bank account information, estimated wealth, identified assets, donation histories, values of donations, and donation recipient organizations;
- d. Medical and health information, including patient and medical record identifiers, treating physician names, medical visit dates, reasons for seeking medical treatment, patient discharge statuses, and health insurance status (*i.e.*, PHI);
- e. Demographic information, including gender, political opinions, and religious beliefs;
- f. Account credentials, including usernames and passwords;
- g. Employment information, including employers, hire dates, annual salaries, and payroll amounts;

---

<sup>34</sup> *Security Incident*, Blackbaud (updated Sept. 29, 2020), <https://www.blackbaud.com/securityincident>.

- h. Marital details, including marital statuses, spouse names, and spouses' giving histories; and
- i. Educational information, including student ID numbers, course and educational attainment details.<sup>35</sup>

37. Had Blackbaud maintained a sufficient security program, including properly monitoring its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud has announced it has “already implemented

---

<sup>35</sup> Form 8-K, *supra* n.25; Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), <https://www.bbc.com/news/technology-53567699> (last visited Mar. 9, 2021); Blackbaud, Inc., Form 8-K Current Report (Sept. 29, 2020), <https://www.sec.gov/ix?doc=/Archives/edgar/data/1280058/000128005820000044/blk-b-20200929.htm> (last visited Mar. 9, 2021); *Blackbaud Security Breach and How It Affects You, Your Privacy and Big Thought*, Big Thought, <https://www.bigthought.org/announcements/news-announcements/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought/> (last visited Mar. 15, 2021) (“In addition, for individuals employed by Big Thought from July 15, 2008 through March 31, 2010, birth date, gender, marital status, hire date, bank name, annual salary and payroll amounts may have been accessed despite being encrypted.”); *Notice to Our Patients of a Privacy Incident*, White Plains Hospital. (Sept. 30, 2020), <https://www.wphospital.org/getmedia/71a84f33-91f4-433b-b34f-116113bed5a2/White-Plains-Substitute-Notice-Draft-FINAL> (“Based on White Plains Hospital’s review of the Blackbaud database involved in the incident, it contained some patient information, including names, addresses, dates of birth, patient identifiers, and potentially in some instances, treating physician names, visit dates, and/or reasons for seeking treatment.”); *Blackbaud Security Incident*, Children’s Minnesota (Sept. 11, 2020), <https://www.childrensmn.org/2020/09/11/blackbaud-security-incident/> (“Based on our investigation and review of the affected Blackbaud database, the incident involved limited patient information that the Foundation received in connection with its fundraising efforts, including: full names, addresses, phone numbers, age, dates of birth, gender, medical record numbers, dates of treatment, locations of treatment, names of treating clinicians and health insurance status.”); *Blackbaud Response*, U. of York (July 21, 2020), <https://www.york.ac.uk/news-and-events/news/2020/blackbaud-response/> (“The data accessed by the cybercriminal may have contained some of the following information: Basic details, [e.g.,] name, title, gender, date of birth and student number (if applicable); Addresses and contact details, [e.g.,] phone, email and LinkedIn profile URL; Course and educational attainment details, [e.g.,] what qualification you received and some of the extracurricular opportunities you participated in while studying at York (if applicable)”; *Blackbaud Security Incident*, Mercy Hosp. & Med. Ctr., <https://www.mercy-chicago.org/blackbaud-incident> (last visited Mar. 15, 2021) (“Other fields were not encrypted and could have been accessible to the cybercriminals including information such as: donor relation to patient, patient discharge status, name of patient insurance and patient department of service, your name, contact information, donation history.”).



changes to prevent this specific issue from happening again.”<sup>36</sup> Had the necessary changes been made previously, this incident would not have happened, and Plaintiffs’ Private Information would not have been accessed.

38. Plaintiffs’ Private Information has been compromised and disclosed to unauthorized third parties because of Blackbaud’s negligent and unlawful conduct—the Private Information that Blackbaud collected and maintained is now in the hands of cybercriminals. Blackbaud cannot reasonably maintain that the data thieves destroyed the extracted data simply because Blackbaud paid the ransom and the perpetrators stated the copy was destroyed. In fact, the Notices provided by the non-profit organizations and educational and other institutions through which Blackbaud obtained Plaintiffs’ data advised that class members should remain aware of suspicious account activity, take further actions such as monitoring their own credit records, and notify the organizations involved and law enforcement authorities of any suspicious activity.<sup>37</sup> Despite this, Blackbaud offered class members little in the way of redress, such as credit monitoring or fraud protection, and provided no financial support for time or expenses incurred as a result of the Data Breach.

39. In response to some of the most egregious instances of stolen data from the Data Breach, Blackbaud has provided minimal support—an offer of two years of single-bureau credit monitoring and “access remediation support” from CyberScout Fraud Investigator for only those

---

<sup>36</sup> *Id.*

<sup>37</sup> For instance, the notice provided to Plaintiff Jessica Case warned that she should “remain vigilant and promptly report any suspicious activity or suspected identity theft to [the non-profit] and to the proper law enforcement authorities, such as the Federal Trade Commission and the Washington State Office of the Attorney General.” Likewise, the notice Plaintiff Kea Molnar received advised her to “remain vigilant and promptly report to [the educational institution] and to the proper law enforcement authorities any suspicious activity or suspected identity theft.”

individuals who had their most sensitive PII taken in unencrypted form, such as SSNs.<sup>38</sup> Some Social Good Entities have also offered identity theft protection services. But those services, standing by themselves, are plainly inadequate: single-bureau monitoring “leaves too much to chance,”<sup>39</sup> and the cybersecurity criminals who stole the data from Blackbaud’s systems will likely attempt to monetize it again.<sup>40</sup> Consequently, Plaintiffs and class members have incurred and will incur out of pocket costs for purchasing their own credit monitoring services or credit reports, or spending money or time on other protective measures as a reasonable solution to deter and detect identity theft.

40. Cybersecurity criminals can also use this data to demand further ransoms from the individuals whose Private Information was stolen off of Blackbaud’s servers. Since Blackbaud already demonstrated to the cybercriminals that the data is valuable enough to extract a ransom, class members face an imminent risk of future harm of paying cybercriminals to protect their information from further disclosure based upon new ransom threats for the same information.<sup>41</sup>

---

<sup>38</sup> In Blackbaud’s letter dated September 29, 2020 to the Kushner School, Blackbaud offered “Identity Theft Protection services to individuals whose Social Security Numbers ... are stored in the areas we described above at no cost to you or the individuals.” Cleve Warren, Executive Director of FSCJ, described that on September 29, 2020, Blackbaud informed the FSCJ Foundation that a back-up file was taken in the ransomware attack and that it contained “certain information that was part of a legacy table of names and Social Security numbers retained on Blackbaud servers that was not encrypted.” <https://www.fscjfoundation.org/Blackbaud.html> (last visited Mar. 26, 2021).

<sup>39</sup> *Should I monitor my credit with one credit bureau or all three? Why it’s better to be thorough if you want to guarantee the best credit possible*, Debt.com (Oct. 28, 2020), <https://www.debt.com/credit-monitoring/three-credit-bureaus/>.

<sup>40</sup> Krebs, *Why Paying to Delete Stolen Data is Bonkers*, *supra* n.1.

<sup>41</sup> *See Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, Coveware (Nov. 4, 2020), <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>.

41. As a result of the Data Breach, Plaintiffs and the class members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud, identity theft, and ransom demands for many years to come. Furthermore, Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and the class members will incur ongoing out-of-pocket costs including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft, among other expenses.

42. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was compromised and disclosed as a result of the Data Breach.

43. Accordingly, Plaintiffs bring this action against Blackbaud seeking redress for its unlawful conduct, and asserting claims for both common law and statutory damages.

### **III. PARTIES**

#### **A. Plaintiffs**

44. Plaintiff Kassandre Clayton is a resident and citizen of California. Plaintiff Clayton is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Clayton's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Clayton would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Clayton's Private Information was compromised and disclosed as a result of the Data Breach.

45. Plaintiff Clayton was required to provide her PHI to several healthcare providers as a predicate to receiving healthcare services. Plaintiff Clayton's PHI was in turn provided to

Blackbaud to be held for safekeeping. In or around September 2020, Plaintiff Clayton received notice from Community Medical Centers that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Clayton's PHI, including, her name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, applicable hospital department or unit had been improperly accessed and/or obtained by unauthorized third parties. Additionally, she received notice from Trinity Health that her name, address, phone number, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name were compromised as a result of the Data Breach.

46. While the notices indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs and any additional medical information, such as diagnosis or treatment plan and/or that certain categories of data were encrypted, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Clayton's was exposed due to Blackbaud's conduct.

47. As a result of the Data Breach, Plaintiff Clayton tried to mitigate its impact after receiving the notification letters, including 2 hours of time spent reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and between 1 and 2 hours monitoring online banking to resolve issues related to the Data Breach. Plaintiff Clayton now spends approximately 3 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 15-20 hours on these tasks, valuable time Plaintiff Clayton otherwise would have spent on other activities, including but not limited to work and/or recreation.

48. Since Plaintiff Clayton was not offered credit monitoring and identity theft protection services by Blackbaud, is an effort to mitigate its impact after receiving the notification letters, she purchased and continues to maintain credit monitoring. Upon receiving notification of the Data Breach, Plaintiff Clayton purchased credit monitoring and identity theft protection services on an annual basis for approximately \$189.95 per year from IdentityProtection.com beginning October 7, 2020. Plaintiff Clayton plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

49. As a result of the Data Breach, Plaintiff Clayton has suffered emotional distress as a result of the release of her Private Information and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Clayton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

50. Plaintiff Clayton suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Clayton; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

51. Moreover, subsequent to the Data Breach, Plaintiff Clayton also experienced actual identity theft and fraud, including notification that her Private Information was found on the dark web and a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

52. Plaintiff Clayton incurred approximately 10 to 15 hours to date, and at least \$189.50 responding to these incidents of attempted identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Clayton otherwise would have spent on other activities, such as work and/or recreation.

53. As a result of the Data Breach, Plaintiff Clayton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Clayton will continue to be at increased risk of identity theft and fraud for years to come.

54. Plaintiff Kathleen Arman is a resident and citizen of Illinois. Plaintiff Arman is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Arman's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Arman would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Arman's Private Information was compromised and disclosed as a result of the Data Breach.

55. Plaintiff Arman was required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services. Plaintiff Arman's PHI was in turn provided to Defendant to be held for safekeeping.

56. In or around September 2020, Plaintiff Arman received notice from NorthShore University Health System ("NorthShore") that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Arman's PHI, including full name, date of birth contact information (address, phone number, email address), admission

and discharge date(s), NorthShore location(s) of services, and physician name(s) and specialties, was compromised as a result of the Data Breach.

57. This notice further indicated that the Data Breach did not involve the exposure of credit card, bank account information, SSNs, user login credentials and passwords. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Arman's was exposed due to Blackbaud's conduct.

58. As a result of the Data Breach, Plaintiff Arman made reasonable efforts to mitigate its impact receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud and freezing her credit. Plaintiff Arman now spends approximately two hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 16 hours on these tasks, valuable time Plaintiff Arman otherwise would have spent on other activities, including but not limited to work and/or recreation.

59. Plaintiff Arman was not offered credit monitoring and identity theft protection services by Blackbaud.

60. As a result of the Data Breach, Plaintiff Arman has suffered emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Arman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

61. Plaintiff Arman suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Arman; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

62. Moreover, subsequent to the Data Breach, Plaintiff Arman also experienced actual identity theft and fraud, including notification that her Private Information was found on the dark web and a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Arman has spent over 20 hours of her time responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Arman otherwise would have spent on other activities, such as work and/or recreation.

63. As a result of the Data Breach, Plaintiff Arman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Arman will continue to be at increased risk of identity theft and fraud for years to come.

64. Plaintiff Sonya Garcia-Martinez is a resident and citizen of Illinois. Plaintiff Garcia-Martinez is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Garcia-Martinez's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Garcia-Martinez would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted



with her Private Information failed to maintain adequate data security. Plaintiff Garcia-Martinez's Private Information was compromised and disclosed as a result of the Data Breach.

65. Plaintiff Garcia-Martinez was required to provide her PHI to OSF HealthCare Foundation as a predicate to receiving healthcare services. Plaintiff Garcia-Martinez's PHI was in turn provided to Blackbaud to be held for safekeeping. This PHI included her contact information, demographic information, date of birth, history of her relationship with OSF HealthCare Foundation.

66. In or around October 2020, Plaintiff Garcia-Martinez received notice from OSF HealthCare Foundation that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Garcia-Martinez's Private Information, including her contact information, demographic information, date of birth, history of her relationship with OSF HealthCare Foundation and other medical information, was compromised as a result of the Data Breach.

67. This notice further indicated that credit card information, bank account information, SSNs and any additional medical information, such as diagnosis or treatment plan, was not accessible because it was encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information or PHI of Plaintiff Garcia-Martinez's was exposed due to the Data Breach.

68. As a result of the Data Breach, Plaintiff Garcia-Martinez made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to, purchasing or continuing to maintain credit monitoring. Plaintiff Garcia-Martinez maintains credit monitoring and identity theft protection from Rival Credit Repair and Experian Credit Monitoring Report for

a monthly total of \$124.99. Additionally, Plaintiff spent 3 to 4 days researching the Data Breach and Blackbaud, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Garcia-Martinez now spends approximately 8 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 4 to 5 days on these tasks, valuable time Plaintiff Garcia-Martinez otherwise would have spent on other activities, including but not limited to work and/or recreation.

69. Plaintiff Garcia-Martinez was not offered credit monitoring and identity theft protection services by Blackbaud, but was offered credit monitoring services from OSF Healthcare. However, Plaintiff Garcia-Martinez found the language of the offer contained in the notification letter confusing and contradictory, since it first encouraged her not to worry, but then offered the monitoring services. She was also uncertain as to whether the offered monitoring services would begin immediately. She thus decided to purchase credit monitoring and identity theft protection services on her own, through Rival Credit Repair and Experian Credit Monitoring Report, on a monthly basis for approximately \$124.99 per month for both providers. Plaintiff Garcia-Martinez plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

70. As a result of the Data Breach, Plaintiff Garcia-Martinez has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information, for purposes of identity theft and fraud. Plaintiff Garcia-Martinez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. She worries daily about her stolen

identity and how it is being used. She is upset at the lack of protection of data. Knowing that she is unable to get a new SSN, she is upset that OSF Healthcare and Blackbaud should have had a better security system in place, especially when dealing with sensitive health and Private Information data.

71. Plaintiff Garcia-Martinez suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Garcia-Martinez; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

72. Moreover, subsequent to the Data Breach, Plaintiff Garcia-Martinez also experienced actual identity theft and fraud, including unusual charges to her accounts in December 2020, including a charge from Cash App for \$290.00 and Microsoft for \$39.95, requiring 3 to 4 days of waiting until reimbursement with a \$0.00 account balance, and 2 weeks until a new debit card was sent to her in the mail. She also noted she unable to withdraw additional funds because her withdrawal limits after the Data Breach increased beyond her ordinary amount, and when she attempted to withdraw funds, her credit union declined her. Additionally, she received notification that Private Information, including her SSN, was found on the dark web; as well as a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

73. Plaintiff Garcia-Martinez spent at least 2 weeks responding to these of identity theft and fraud as a result of the Data Breach, 4 days of which she had to incur without access to any funds, nor her cell phone because her prepaid minutes expired during the period wherein she was without access to funds, and was unable to purchase additional minutes during this time. The time

spent dealing with these resulting from the Data Breach is time Plaintiff Garcia-Martinez otherwise would have spent on other activities, such as work and/or recreation.

74. As a result of the Data Breach, Plaintiff Garcia-Martinez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Garcia-Martinez will continue to be at increased risk of identity theft and fraud for years to come.

75. Plaintiff Joseph I. Frontera is a resident and citizen of Maryland. Plaintiff Frontera is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Frontera's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Frontera would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Frontera's Private Information was compromised and disclosed as a result of the Data Breach.

76. Plaintiff Frontera was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Frontera's PHI was in turn provided to Defendant to be held for safekeeping.

77. In or around September 2020, Plaintiff Frontera received notice from Mercy Health Services that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Frontera's PHI, including name, date of birth, certain information relating to health visits to Mercy such as dates and times of those visits, and physicians or departments that provided him with care, was compromised as a result of the Data Breach.

78. This notice further indicated that the Data Breach did not involve the exposure of information such as SSNs or financial card information and/or that certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Frontera's was exposed due to Blackbaud's conduct.

79. As a result of the Data Breach, Plaintiff Frontera made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Frontera now spends approximately one to two hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff Frontera has spent at least 30 hours on these tasks, valuable time Plaintiff Frontera otherwise would have spent on other activities, including but not limited to work and/or recreation.

80. Plaintiff Frontera was not offered credit monitoring and identity theft protection services by Blackbaud.

81. As a result of the Data Breach, Plaintiff Frontera has suffered emotional distress as a result of the release of his PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Frontera is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

82. Plaintiff Frontera suffered actual injury from having his PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PHI, a form of property that Blackbaud obtained from Plaintiff Frontera; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

83. Moreover, subsequent to the Data Breach, Plaintiff Frontera also experienced actual identity theft and fraud. Plaintiff Frontera has replaced his credit cards twice since the breach as a result of unauthorized credit card purchases at gas stations and mini marts. Credit cards for Neiman Marcus and Helzberg Diamond had been fraudulently opened in his name with charges in excess of \$10,000. In response to these fraudulent charges, Plaintiff Frontera filed a police report. Plaintiff Frontera was in the process of refinancing his home when an “unpaid” notification showed up on his credit report from the Helzberg Diamond fraudulent charge. Plaintiff Frontera has received scam emails from PayPal and Amazon notifying him that he needs to reset his account or verify information or these accounts will be closed. In addition, Plaintiff Frontera received notification that his Private Information was found on the dark web; has experienced an increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

84. Plaintiff Frontera has spent approximately ten hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Frontera otherwise would have spent on other activities, such as work and/or recreation.

85. As a result of the Data Breach, Plaintiff Frontera anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Frontera will continue to be at increased risk of identity theft and fraud for years to come.

86. Plaintiff Angela Maher is a resident and citizen of Michigan. Plaintiff Maher is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Maher's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Maher would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Maher's Private Information was compromised and disclosed as a result of the Data Breach.

87. Plaintiff Maher was required to provide her PHI to her healthcare provider as a predicate to receive healthcare services. Plaintiff Maher's PHI was in turn provided to Blackbaud to be held for safekeeping.

88. In or around September, 2020, Plaintiff Maher received notice from Trinity Health that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Maher's PHI, including patient discharge status, patient insurance, patient department of service, full name, address, phone numbers, email, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name, was compromised as a result of the Data Breach.

89. The notice further indicated that the Data Breach did not involve certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Maher's was exposed due to Blackbaud's conduct.

90. As a result of the Data Breach, Plaintiff Maher made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services. Plaintiff Maher now spends approximately 2 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Maher otherwise would have spent on other activities, including but not limited to work and/or recreation.

91. As a result of the Data Breach, Plaintiff Maher has suffered emotional distress as a result of the release of her PHI which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Maher is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

92. Plaintiff Maher suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Maher; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

93. Moreover, subsequent to the Data Breach, Plaintiff Maher also experienced actual identity theft and fraud. Plaintiff Maher had at least 3 unauthorized charges on her debit card that were small dollar amounts from other countries. She had to cancel her debit card at least 2 times and each time she received a new card, that card was declined when she tried to use it for purchases.



Subsequently, she cancelled her debit card completely. Plaintiff Maher was charged a \$45 fee for a late payment on her Costco/Visa card because her compromised debit card was used for automatic bill payments for her Costco/Visa card. As a result, her Costco/Visa card was cancelled permanently. Plaintiff Maher is aware that her Private Information was found on the dark web as well. In addition, Plaintiff Maher has experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails which she spends dozens of hours dealing with and trying to rectify.

94. Plaintiff Maher has spent approximately over 120 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Maher otherwise would have spent on other activities, such as work and/or recreation.

95. As a result of the Data Breach, Plaintiff Maher anticipates spending considerable time as needed to try to mitigate and address harms caused by the Data Breach. Plaintiff Maher will continue to be at increased risk of identity theft and fraud for years to come.

96. Plaintiff Ralph Peragine is a resident and citizen of New York. Plaintiff Peragine is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Peragine's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Peragine would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Peragine's Private Information was compromised and disclosed as a result of the Data Breach.

97. Plaintiff Peragine was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Peragine's PHI was in turn provided to Blackbaud to be held for safekeeping.

98. In or around October 2020, Plaintiff Peragine received notice from New Haven Hospital that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Peragine's PHI, including name, address, phone number, date of birth, philanthropic history, name of doctor and dates of service at the hospital, was compromised as a result of the Data Breach.

99. This notice further indicated that the Data Breach did not involve the exposure of bank accounts, credit cards, SSNs, and/or that certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII of Plaintiff Peragine's was exposed due to Blackbaud's conduct.

100. As a result of the Data Breach, Plaintiff Peragine made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Peragine now spends approximately 30 minutes per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least three hours on these tasks, valuable time Plaintiff Peragine otherwise would have spent on other activities, including but not limited to work and/or recreation.

101. Plaintiff Peragine was not offered credit monitoring and identity theft protection services by Blackbaud.

102. As a result of the Data Breach, Plaintiff Peragine has suffered emotional distress as a result of the release of his Private Information, including PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Peragine is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

103. Plaintiff Peragine suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Blackbaud obtained from Plaintiff Peragine; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

104. Moreover, subsequent to the Data Breach, Plaintiff Peragine also experienced actual identity theft and fraud. Someone applied for and received unemployment benefits in Plaintiff Peragine's name. Plaintiff Peragine filed a notice on the New York Department of Labor website indicating that he had not applied for unemployment benefits. Plaintiff Peragine spent approximately one hour responding to this incident of identity theft and fraud as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Peragine otherwise would have spent on other activities, such as work and/or recreation.

105. As a result of the Data Breach, Plaintiff Peragine anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Peragine will continue to be at increased risk of identity theft and fraud for years to come.

106. Plaintiff Michele Pettiford is a resident and citizen of Ohio. Plaintiff Pettiford is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and

continues to maintain Plaintiff Pettiford's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Pettiford would not have entrusted her Private Information to one or more Social Good Entities had her known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Pettiford's Private Information was compromised and disclosed as a result of the Data Breach.

107. In or around September 2020, Plaintiff Pettiford received notice from the Smithsonian Institution that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Pettiford's PII including demographic information such as names, U.S. addresses, phone numbers, and summary of donations, was compromised as a result of the Data Breach.

108. This notice further indicated that the Data Breach did not involve the exposure of any credit card information, SSNs, banking information or other similar data. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII of Plaintiff Pettiford's was exposed due to Blackbaud's conduct.

109. As a result of the Data Breach, Plaintiff Pettiford made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: purchasing or maintaining credit monitoring services; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Pettiford now spends approximately ten hours per month reviewing credit monitoring reports and/or checking account statements for irregularities since the data breach to present. This is valuable time Plaintiff

Pettiford otherwise would have spent on other activities, including but not limited to work and/or recreation.

110. Since Plaintiff Pettiford was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Pettiford has elected to maintain credit monitoring and identity theft protection services on a monthly basis for approximately \$24.95 per month. Plaintiff Pettiford plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

111. As a result of the Data Breach, Plaintiff Pettiford has suffered emotional distress resulting from the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Pettiford is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

112. Plaintiff Pettiford suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Pettiford; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

113. Moreover, subsequent to the Data Breach, Plaintiff Pettiford also experienced actual identity theft and fraud. An unknown individual fraudulently applied for unemployment benefits in her name and received \$14,280. In order to fix the issue, Plaintiff Pettiford had to call the unemployment office where she was instructed to file a fraud charge on the government website. In addition, Plaintiff Pettiford had two unauthorized attempted charges on her American

Express card and has received notifications that her PII information was found on the dark web. Plaintiff Pettiford has also experienced a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

114. Plaintiff Pettiford has spent approximately 80 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Pettiford otherwise would have spent on other activities, such as work and/or recreation.

115. As a result of the Data Breach, Plaintiff Pettiford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Pettiford will continue to be at increased risk of identity theft and fraud for years to come.

116. Plaintiff Theresa Welsh is a resident and citizen of Oregon. Plaintiff Welsh is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Welsh's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Welsh would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Welsh's Private Information was compromised and disclosed as a result of the Data Breach.

117. In or around July, 2020, Plaintiff Welsh received notice from Children's Cancer Association that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Welsh's PII, including information pertaining to her relationship with Children's Cancer Association, was compromised as a result of the Data Breach.

118. The Children's Cancer Association notice further indicated that the Data Breach did not involve credit card information, SSNs, bank account information, usernames, or passwords because they were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Welsh's was exposed due to Blackbaud's conduct.

119. As a result of the Data Breach, Plaintiff Welsh made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: purchasing or continuing to maintain credit monitoring services and continuing to monitor all of her accounts on a daily basis. To date, Plaintiff Welsh has spent at least 10 hours on these tasks, valuable time Plaintiff Welsh otherwise would have spent on other activities, including but not limited to work and/or recreation.

120. Since Plaintiff Welsh was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Welsh will continue paying for credit monitoring through Geico at a cost of approximately \$80 per year. Plaintiff Welsh plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

121. As a result of the Data Breach, Plaintiff Welsh has suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Welsh is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

122. Plaintiff Welsh suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Welsh; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

123. Moreover, subsequent to the Data Breach, Plaintiff Welsh also experienced actual identity theft and fraud, including an unauthorized charge on a payment card, information found on the dark web and at least 20 suspicious, unsolicited phishing telephone calls a day, from the date of the Data breach and continues to the present. These unsolicited telephone calls are a tremendous disruption and interference with her job as a trainer/presenter since she is required to keep her phone on while teaching.

124. Plaintiff Welsh has spent at least 10 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Welsh otherwise would have spent on other activities, such as work and/or recreation.

125. As a result of the Data Breach, Plaintiff Welsh anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Welsh will continue to be at increased risk of identity theft and fraud for years to come.

126. Plaintiff Latricia Ford is a resident and citizen of South Carolina. Plaintiff Ford is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Ford's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Ford would not



have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Ford's Private Information was compromised and disclosed as a result of the Data Breach.

127. Plaintiff Ford was required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services. Plaintiff Ford's PHI was in turn provided to Defendant to be held for safekeeping.

128. In or around September 2020, Plaintiff Ford received notice from Roper St. Francis Healthcare that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Ford's PHI, including name, gender, date of birth, address, date(s) of treatment, department(s) of service, and treating physician(s) were compromised as a result of the Data Breach.

129. This notice further indicated that the Data Breach did not involve the exposure of SSNs, financial account information, credit card information, or electronic health records. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PHI of Plaintiff Ford's was exposed due to Blackbaud's conduct.

130. As a result of the Data Breach, Plaintiff Ford made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing explanation of benefit statements from health care providers for which Plaintiff Ford spends approximately one hour per month reviewing these statements for irregularities. To date, Plaintiff Ford has spent at least six hours on these tasks, valuable time Plaintiff Ford otherwise would have spent on other activities, including but not limited to work and/or recreation.

131. Plaintiff Ford was not offered credit monitoring and identity theft protection services by Blackbaud.

132. As a result of the Data Breach, Plaintiff Ford has suffered emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Ford is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

133. Plaintiff Ford suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Ford; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

134. Moreover, subsequent to the Data Breach, Plaintiff Ford also experienced actual fraud and identity theft, including an increase in suspicious emails and phone calls. Plaintiff Ford has received numerous cyber alerts from MyIDCare where she was informed that individuals had gained knowledge of her name, email, previous home address and telephone number. Plaintiff Ford received a fraudulent phone call from someone impersonating her internet provider who attempted to gain access to her work computer; and has also been notified that someone had requested an insurance quote in her name from State Farm Insurance for a vehicle Plaintiff Ford does not own and in connection with this request for an insurance quote, State Farm did a soft inquiry on her credit.

135. Plaintiff Ford spent approximately four hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents

resulting from the Data Breach is time Plaintiff Ford otherwise would have spent on other activities, such as work and/or recreation.

136. As a result of the Data Breach, Plaintiff Ford anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Ford will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff Clifford Scott is a resident and citizen of South Carolina. Plaintiff Scott is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Scott's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Scott would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with him Private Information failed to maintain adequate data security. Plaintiff Scott's Private Information was compromised and disclosed as a result of the Data Breach.

138. Plaintiff Scott was required to provide his PII to entities to whom he made charitable donations. Plaintiff Scott's PII was in turn provided to Defendant to be held for safekeeping.

139. In or around September 2020, Plaintiff Scott received notice from the University of South Carolina that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Scott's PII, including name, contact information, demographic information, date of birth and giving profiles and history were compromised as a result of the Data Breach.

140. As a result of the Data Breach, Plaintiff Scott made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing financial

account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Scott spends at least 2 hours per month reviewing these statements for irregularities. This is valuable time Plaintiff Scott otherwise would have spent on other activities, including but not limited to work and/or recreation.

141. Plaintiff Scott was not offered credit monitoring and identity theft protection services by Blackbaud.

142. As a result of the Data Breach, Plaintiff Scott has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Scott is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach

143. Plaintiff Scott suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Blackbaud obtained from Plaintiff Scott; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

144. Moreover, subsequent to the Data Breach, Plaintiff Scott also experienced actual fraud, including an increase in suspicious text messages and phone calls. In addition, Plaintiff Scott's email and phone number have been found on the dark web. Plaintiff Scott has spent numerous hours responding to these incidents of identity theft and fraud as a result of the Data Breach and dealing with the Data Breach in general. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Scott otherwise would have spent on other activities, such as work and/or recreation.

145. As a result of the Data Breach, Plaintiff Scott anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Scott will continue to be at increased risk of identity theft and fraud for years to come.

146. Plaintiff Robert Watts, Jr. is a resident and citizen of Texas. Plaintiff Watts is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Watts' Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Watts would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Watts' Private Information was compromised and disclosed as a result of the Data Breach.

147. Plaintiff Watts was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Watts' PHI was in turn provided to Defendant to be held for safekeeping.

148. In or around August 17, 2020, Plaintiff Watts received notice from UTHealth that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Watt's PHI, including his name and address, was compromised as a result of the Data Breach.

149. This notice further indicated that the Data Breach did not involve exposure of sensitive data-such as SSNs, credit card information or bank account information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Watts was exposed due to Blackbaud's conduct.

150. As a result of the Data Breach, Plaintiff Watts made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Watts now spends approximately 3 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 30 hours dealing with this Data Breach, valuable time Plaintiff Watts otherwise would have spent on other activities, including but not limited to work and/or recreation.

151. Since Plaintiff Watts was not offered credit monitoring and identity theft protection services by Blackbaud.

152. As a result of the Data Breach, Plaintiff Watts has suffered emotional distress as a result of the release of his PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Watts is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

153. Plaintiff Watts suffered actual injury from having his PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PHI, a form of property that Blackbaud obtained from Plaintiff Watts; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

154. Moreover, subsequent to the Data Breach, Plaintiff Watts also experienced actual identity theft and fraud, including unauthorized charges of approximately between \$1,200-\$1,400 on his credit card as well as a significant increase in suspicious, unsolicited phishing phone calls

and emails. Plaintiff Watts traveled to his bank in order to replace his compromised credit card. In addition, he performed his own investigation into the fraudulent credit card purchases, had communication with the Federal Bureau of Investigation (“FBI”) regarding these charges and filed a police report. Plaintiff Watts had to spend time resetting automatic billing instructions tied to his compromised account and has spent at least 16 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Watts otherwise would have spent on other activities, such as work and/or recreation.

155. As a result of the Data Breach, Plaintiff Watts anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Watts will continue to be at increased risk of identity theft and fraud for years to come.

156. Plaintiff Jason Money is a resident and citizen of Virginia. Plaintiff Money is acting on his own behalf, and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Money’s Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Money would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity’s primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Money’s Private Information was compromised and disclosed as a result of the Data Breach.

157. Plaintiff Jason Money was required to provide his PHI to his healthcare provider as a predicate for him to receive healthcare services. Plaintiff Money’s PHI was in turn provided to Blackbaud to be held for safekeeping.

158. In or around September, 2020, Plaintiff Money received notice from Inova Health System that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Money's PHI, including his name, address, date of birth, phone number, provider name(s), date(s) of service, and/or hospital department(s), philanthropic giving history, such as donation dates and amounts, was compromised as a result of the Data Breach.

159. This notice further indicated that the Data Breach did not impact his SSN, which Inova claims they do not collect or his financial account information and/or payment card information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Money was exposed due to Blackbaud's conduct.

160. As a result of the Data Breach, Plaintiff Money made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Money now spends approximately 30 minutes a day reviewing his credit card statements, bank accounts, home equity line of credit and credit monitoring reports for irregularities. To date, Plaintiff Money has spent at least 150 hours on these tasks, valuable time Plaintiff Money otherwise would have spent on other activities, including but not limited to work, caring for his wife and/or recreation.

161. Plaintiff Money was not offered credit monitoring and identity theft protection services by Blackbaud.

162. As a result of the Data Breach, Plaintiff Money has suffered significant emotional distress as a result of the release of his PHI, which he believed would be protected from



unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Money is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

163. Plaintiff Money suffered actual injury from having his PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PHI, a form of property that Blackbaud obtained from Plaintiff Money; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

164. Moreover, subsequent to the Data Breach, Plaintiff Money also experienced actual identity theft and fraud, including multiple unauthorized charges totaling approximately \$200 on his credit card; he received alerts that his Private Information was found on the dark web, and has a significant increase in the amount of suspicious, unsolicited phishing telephone calls, which includes up to 4-5 robocalls per day; and emails related to medical companies for medical services and medical products. Plaintiff Money has spent dozens of hours responding to these incidents of identity theft and fraud as a result of the Data Breach including resetting automatic billing instructions on at least eight accounts that were tied to his compromised account. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Money otherwise would have spent on other activities, such as work, caring for his wife and/or recreation.

165. As a result of the Data Breach, Plaintiff Money anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Money will continue to be at increased risk of identity theft and fraud for years to come.

166. Plaintiff Nicole Money is a resident and citizen of Virginia. Plaintiff Nicole Money's husband Jason Money is acting on her behalf and on behalf of others similarly situated, as Plaintiff Money is a quadriplegic and non-verbal. Blackbaud obtained and continues to maintain Plaintiff Money's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Money would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Money's Private Information was compromised and disclosed as a result of the Data Breach.

167. Plaintiff Nicole Money was required to provide her PHI to her healthcare provider as a predicate for her to receive healthcare services. Plaintiff Money's PHI was in turn provided to Blackbaud to be held for safekeeping.

168. In or around September, 2020, Plaintiff Money received notice from Inova Health System that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Money's PHI, including her name, address, date of birth, phone number, provider name(s), date(s) of service, and/or hospital department(s), philanthropic giving history, such as donation dates and amounts, was compromised as a result of the Data Breach.

169. This notice further indicated that the Data Breach did not impact her SSN, which Inova claims they do not collect or her financial account information and/or payment card information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Money was exposed due to Blackbaud's conduct.

170. As a result of the Data Breach, Plaintiff Money's husband made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records and medical claim forms for any indications of actual or attempted identity theft or fraud. Plaintiff Money's husband now spends approximately 30 minutes a day reviewing her credit card statements, bank accounts, home equity line of credit and credit monitoring reports for irregularities. To date, Plaintiff Money's husband has spent at least 150 hours on these tasks, valuable time Plaintiff Money's husband otherwise would have spent on other activities, including but not limited to work, caring for Plaintiff Money and/or recreation.

171. Plaintiff Money was not offered credit monitoring and identity theft protection services by Blackbaud.

172. As a result of the Data Breach, Plaintiff Money and her husband have suffered significant emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Money is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach especially given the fact that Plaintiff Money receives 24/7 medical care and it is extremely important that there is no interference with this care as a consequence of the Data Breach.

173. Plaintiff Money suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Money; (b) violation of her privacy

rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

174. Moreover, subsequent to the Data Breach, Plaintiff Money also experienced actual identity theft and fraud, including an unauthorized credit card opened in her name that Plaintiff Money did not apply for and a fraudulent PayPal account opened in her name. Plaintiff Money's husband has spent 5 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Money's husband otherwise would have spent on other activities, such as work, caring for Plaintiff Money and/or recreation.

175. As a result of the Data Breach, Plaintiff Money anticipates that her husband will be spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Money will continue to be at increased risk of identity theft and fraud for years to come.

## **B. Defendant**

176. Defendant Blackbaud, Inc. is a Delaware corporation with its principal place of business located at 65 Fairchild Street, Charleston, South Carolina. Blackbaud's common stock is publicly traded on the NASDAQ under the ticker symbol "BLKB." Blackbaud manages, maintains, and provides cloud computing software, services, and cybersecurity for clients including healthcare organizations, education institutions, and other non-profit corporations,<sup>42</sup> including the non-profits which obtained and maintained Plaintiffs' Private Information that was

---

<sup>42</sup> See *About Blackbaud*, Blackbaud, <https://www.blackbaud.com/company> (last visited Mar. 15, 2021).

compromised in the Data Breach. Blackbaud has “over 45,000 customers located in over 100 countries.”<sup>43</sup>

#### **IV. JURISDICTION AND VENUE**

177. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1711, et seq., because at least one member of the Class, as defined below, is a citizen of a different state than Blackbaud, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

178. This Court has personal jurisdiction over this action because Blackbaud maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. See 28 U.S.C. § 1332(a).

179. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Blackbaud’s principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

#### **V. STATEMENT OF FACTS**

##### **A. A Sophisticated Cloud-Service Provider, Blackbaud Knew of the Risk That Cybercriminals Posed to Hosted Data**

180. Incorporated in 1982, Blackbaud describes itself as “the world’s leading cloud software company powering social good.”<sup>44</sup> It provides “cloud software, services, expertise and

---

<sup>43</sup> 2019 Form 10-K, *supra* n.11.

<sup>44</sup> 2019 Form 10-K, *supra* n.11.

data intelligence,” which its clients use for administration, fundraising, and financial management.<sup>45</sup>

181. Blackbaud is a publicly-traded company with clients that include “nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them.”<sup>46</sup> Blackbaud specifically markets its products to these entities, noting the robust data security policies and protections it has in place to safeguard the Private Information of donors, students, congregants, and patients. The Social Good Entities process sensitive information about individuals’ financial status, health, and/or educational background in order to perform their missions and raise money.

182. This marketing has proved to be a lucrative business for Blackbaud, which reported that, “[a]t the end of 2019, [it] had over 45,000 customers located in over 100 countries[,]” with a “total addressable market (“TAM”) . . . greater than \$10 billion.”<sup>47</sup> Blackbaud’s business depends upon the need to process and keep safe the Private Information of millions of individuals every day.

183. In the ordinary course of doing business with Blackbaud’s clients, individuals are regularly required to provide Private Information that is collected, stored, maintained, and secured by Blackbaud.

184. This information is valuable and requires someone to provide security; without this Private Information, there is no Blackbaud.

---

<sup>45</sup> *Id.*

<sup>46</sup> *Supra* n.42.

<sup>47</sup> 2019 Form 10-K, *supra* n.11, at 3.

185. Blackbaud collects and stores Private Information from individuals, for which Blackbaud is paid. Blackbaud derives a “significant portion” of its revenue from “transaction-based payment processing fees” that it collects from its customers through the Blackbaud Merchant Services solution, which enables Blackbaud’s customers’ donors to make donations and purchase goods and services using various payment options.<sup>48</sup> Indeed, based upon the undersigned’s investigation, the more Private Information is housed on its servers, the more Blackbaud charges. In offering and marketing its products, Blackbaud solicits and obtains Private Information of Plaintiffs and class members from the Social Good Entities for storage on its servers and data analysis. In so doing, Blackbaud offers dedicated services to Social Good Entities, and a significant component and selling point of these services is data security to protect this high-value Private Information.

186. Blackbaud offers a number of solutions and services to power what it purports to be “the world’s most robust philanthropic data set.”<sup>49</sup> The solutions offered by Blackbaud include fundraising and relationship management, marketing and engagement, financial management, grant and award management, organizational and program management, social responsibility, payment services, and analytics.<sup>50</sup> The Blackbaud portfolio is “delivered primarily through cloud solutions.”<sup>51</sup>

187. The specific solutions offered by Blackbaud are named Blackbaud’s Raiser’s Edge NXT®; Blackbaud CRM™; Blackbaud eTapestry®; Blackbaud TeamRaiser®; Blackbaud Peer-to-Peer Fundraising™, powered by JustGiving™; Blackbaud Guided Fundraising™ and

---

<sup>48</sup> 2020 Form 10-K, *supra* n.11, at 18.

<sup>49</sup> *Id.* at 7.

<sup>50</sup> *Id.* at 7-10.

<sup>51</sup> *Id.*

Blackbaud Volunteer Network Fundraising™; Blackbaud Luminate Online®; Blackbaud Online Express™; Blackbaud School Website System™; Blackbaud Financial Edge NXT®; Blackbaud Tuition Management™; Blackbaud Financial Aid Management™; Blackbaud Grantmaking™; Blackbaud Award Management™; Blackbaud Student Information System™; Blackbaud Learning Management System™; Blackbaud Enrollment Management System™; Blackbaud Altru®; Blackbaud Church Management™; YourCause® Grants Connect® and YourCause CSR Connect®; Blackbaud Merchant Services™; Blackbaud Purchase Cards; and Blackbaud Intelligence for Good®.<sup>52</sup>

188. Two of Blackbaud’s most popular products include “Blackbaud Raiser’s Edge NXT” and “Blackbaud Financial Edge NXT.”<sup>53</sup> With Blackbaud Financial Edge NXT®, Blackbaud uses “advanced technology with powerful reporting tools to help accounting teams drive transparency, stewardship, and compliance while enabling them to seamlessly manage transactions and eliminate manual processes.” It also integrates with Blackbaud’s Raiser’s Edge NXT to “simply gift entry processing and relates information from both systems in an informative manner to eliminate redundant tasks and manual processes.”<sup>54</sup>

189. Blackbaud determines the purposes or means of processing customers’ data based on which solutions or services are utilized by the customers. Blackbaud has specific means by which it processes payments using Blackbaud Raiser’s Edge NXT®, Blackbaud Tuition Management™, Blackbaud Merchant Services™, Blackbaud Purchase Cards, and other tools. Blackbaud describes its payment services as providing its customers “payment processing abilities

---

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 7, 8.

<sup>54</sup> *Id.*



that enable their donors to make donations and purchase goods and services using numerous payment options, including credit card and automated clearing house (“ACH”) checking transactions, through secure online transactions.”<sup>55</sup>

190. It also has specific means by which it processes gifts using Blackbaud eTapestry®, Blackbaud Luminate Online®, and Blackbaud Financial Edge NXT®.<sup>56</sup>

191. Blackbaud also has a specific “intuitive and streamlined application process” it uses for purposes of Blackbaud Award Management™ and a simplified system of sharing student data and academic records securely that it uses in its Blackbaud Student Information System™.<sup>57</sup>

192. In addition to these services, Blackbaud has professional and managed services in which its expert consultants provide data conversion, implementation, and customization services for each of its software solutions, including system implementation; data conversion, business process analysis and application customization; database merging and enrichment, and secure credit card transaction processing; database production activities; and website design services.<sup>58</sup> In addition, Blackbaud provides consulting services to advise customers on how to improve a business process.<sup>59</sup>

193. Blackbaud also touts its Customer Success organization, which “develops and fosters relationships within all levels of the customer organization to build more demonstrated value in [Blackbaud’s] solutions and services, while helping customers achieve their desired

---

<sup>55</sup> *Id.*

<sup>56</sup> *Id.* at 7-10.

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

<sup>59</sup> *Id.*

outcomes.”<sup>60</sup> Blackbaud has Customer Success Managers that work with customers to collect and analyze actionable information through direct customer relationships or aggregated analytics that drives future one-to-one or one-to-many interactions. The goal of the Customer Success organization is to “partner with customers to ensure that they are full engaged and have an advocate at Blackbaud who works with them to meet their needs.”<sup>61</sup>

194. In addition to its Customer Success organization, Blackbaud offers customer support and maintenance, which includes up-to-date regular communications, around-the-clock support resources, and Blackbaud’s extensive knowledgebase and forums. Blackbaud also claims to apply its “industry knowledge and experience, combined with expert knowledge of [its] solutions, to evaluate an organization’s needs and consult on how to improve a business process.”<sup>62</sup>

195. Despite Blackbaud’s self-representation as a data security company, it has a deficient security program and no means to effectively manage or govern the data it holds. There are a number of known instances where Blackbaud maintained unencrypted Private Information. For example, the document ID field in Financial Edge NXT for I9 data was not encrypted.<sup>63</sup> This data field included, inter alia, SSNs, driver’s license numbers, and passport numbers.<sup>64</sup> Additional unencrypted information, including credit card information, was also accessible from Raiser’s

---

<sup>60</sup> *Id.* at 10.

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> See Build Consulting, *Blackbaud Cybersecurity Incident: You’re your Organization Needs to Know*, <https://buildconsulting.com/learning/blackbaud-cybersecurity-incident-response-options/> (last visited Mar. 29, 2021).

<sup>64</sup> *Id.*

Edge NXT and a system table from the Education Edge solution.<sup>65</sup> Blackbaud has also acknowledged that prior versions of its products, like Blackbaud CRM, stored unencrypted cardholder data.<sup>66</sup> Blackbaud also maintained unencrypted Private Information of some individuals on legacy versions of programs which were no longer in active use. Blackbaud knew this information was (a) unencrypted and thus subject to breach and misuse; (b) could not be seen by the Social Good Entities; (c) included highly sensitive PII; and (d) was “at rest,” meaning the data was not in transit and being actively used. The failure to encrypt this “at rest” obsolete data containing highly sensitive PII on legacy and/or back-up versions of Blackbaud systems was particularly flagrant and egregious. There was no valid reason for retaining this highly sensitive PII, including SSNs, and Blackbaud’s lax treatment of this PII made public exposure in a cyberattack very likely. Blackbaud has, in fact, acknowledged its failure to encrypt this highly sensitive PII which was “at rest,” and only after the breach has embarked on a program to encrypt such data.<sup>67</sup>

196. The data security component of Blackbaud’s services is of great value to Social Good Entities, and the Social Good Entities pay a premium for this component of Blackbaud’s services. Many of the Social Good Entities depend largely or wholly upon voluntary donations, and any concerns by donors as to the security of their Private Information can have significant adverse economic impacts, including a substantial decrease in donations. This is particularly true

---

<sup>65</sup> Blackbaud, *How are credit cards imported in version 7.91 and higher*, <https://kb.blackbaud.com/articles/Article/51196> (last visited Mar. 29, 2021).

<sup>66</sup> Blackbaud, *PA DSS Implementation for Blackbaud CRM*, <https://www.blackbaud.com/files/support/guides/enterprise/400/padsscrm40sp7.pdf> (last visited Mar. 29, 2021).

<sup>67</sup> See Paul Clolery, *Some Donor Data Accessed in Blackbaud Hack*, NonProfit Times (Sept. 29, 2020), [https://www.thenonproffitimes.com/npt\\_articles/breaking-some-donor-data-accessed-in-blackbaud-hack/](https://www.thenonproffitimes.com/npt_articles/breaking-some-donor-data-accessed-in-blackbaud-hack/).

now, when many of the Social Good Entities are especially vulnerable on account of the widespread economic impacts of the ongoing pandemic.

197. At all relevant times, Blackbaud knew the Private Information stored on its computer systems was valuable and at risk of cyberattack. In its 2019 Annual Report, Blackbaud specifically acknowledged the risk of cyberattacks. Specifically, Blackbaud stated:

If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.

Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.<sup>68</sup>

198. Further, Blackbaud acknowledged the sophistication of attacks and the need to constantly evaluate and adjust its procedures:

Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue. Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely. As these threats continue to evolve and increase, we may be required to devote significant additional resources in order to modify and enhance our security controls and to identify and remediate any security vulnerabilities.<sup>69</sup>

199. As such, Blackbaud identified the risk of failing to detect an attack and the consequences of such a failure, including a failure to respond adequately or on a timely basis.

---

<sup>68</sup> *Id.* at 20.

<sup>69</sup> *Id.*

Additionally, Blackbaud identified risks inherent in a data breach and duties such a breach would trigger.

A compromise of our data security that results in customer or donor personal or payment card data being obtained by unauthorized persons could adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties. We might be required to expend significant capital and other resources to further protect against security breaches or to rectify problems caused by any security breach, including notification under data privacy laws and regulations and expenses related to remediating our information security systems. Even though we carry cyber-technology insurance policies that may provide insurance coverage under certain circumstances, we might suffer losses as a result of a security breach that exceed the coverage available under our insurance policies or for which we do not have coverage. A security breach and any efforts we make to address such breach could also result in a disruption of our operations, particularly our online sales operations.<sup>70</sup>

200. Although Blackbaud identified these risks as its own, it demonstrates an acute awareness of the adverse effects that could result from a data breach. Blackbaud recognized that it had a duty to keep Private Information secure.

Further, the existence of vulnerabilities, even if they do not result in a security breach, may harm client confidence and require substantial resources to address, and we may not be able to discover or remedy such security vulnerabilities before they are exploited, which may harm our business, reputation and future financial results.<sup>71</sup>

201. The risk that data breaches and ransomware could cause to any business was well-known throughout the cybersecurity industry. The Identity Theft Resource Center identified ransomware as the “preferred method of data theft” by cyberthieves,<sup>72</sup> and the FTC cautioned

---

<sup>70</sup> *Id.*

<sup>71</sup> *Id.*

<sup>72</sup> *Identity Theft Resource Center 2020 Annual Report*, <https://notified.idtheftcenter.org/s/>.

businesses that developing a cybersecurity plan and educating employees is the best way to combat such attacks.<sup>73</sup>

202. The importance of developing a cybersecurity plan is more acute now than ever, as data breaches and ransomware attacks become more prevalent.<sup>74</sup> Accordingly, Blackbaud was on notice of the harms that could ensue if it failed to protect individuals' Private Information.

203. Blackbaud itself knew that cyberattacks were a problem for businesses, and frequently informed its customers about the risks that companies faced as a result. Blackbaud recommended that its customers develop a "cybersecurity strategy that will combat cyberattacks and empower staff to become cyber security experts" to avoid the significant costs of data breaches:

---

<sup>73</sup> *Cybersecurity for Small Business: Ransomware*, Federal Trade Commission, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last visited Mar. 28, 2021).

<sup>74</sup> *Healthcare Data Breach Statistics*, HIPAA Journal, <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last visited Mar. 28, 2021) ("Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").



204. Blackbaud cautioned that its customers could face significant risk of the “exposure of data / personal identity information” in the event of a data breach, as well as the threat of ransomware. Blackbaud recommended that clients build out controls to guard against these risks.

.....

### Developing a Cyber Security Strategy

First, map out your threats and risks. Imagine what your worst-case scenario would look like. This could include theft of money (access to your bank accounts, wire fraud), exposure of data / personal identity information (student, donor, or employee records), availability of critical systems, theft of resources (for money), or ransomware.

Second, build out key controls. Now that you have a clear understanding of what you're trying to stop, lay out the controls that relate—combating phishing, protecting credentials, etc. Create initial controls against your top risks. For those that own or govern programs, leverage industry frameworks like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF).

76

<sup>75</sup> *Fighting Cyber Crime: Its Not Just a Job for IT*, Blackbaud (Sept. 2019), [https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/cyber-security.pdf?sfvrsn=61aa0bb\\_0](https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/cyber-security.pdf?sfvrsn=61aa0bb_0).

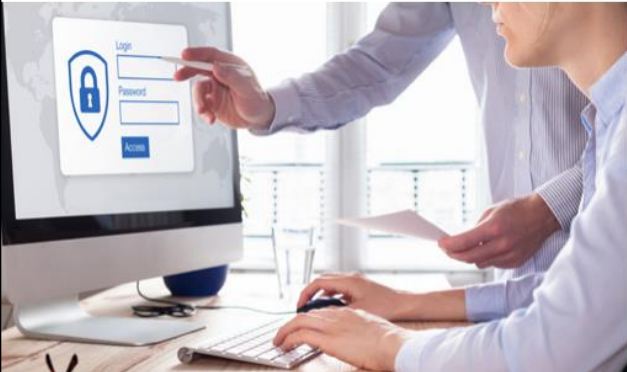
<sup>76</sup> *Id.*

205. Based upon their significant expertise, Blackbaud warned consumers that managing data, knowing what data customers had, ensuring that vendors perform due diligence on their systems, and encrypting data were—among other things—the best way to safeguard data.

### 7 Key Focus Areas to Optimize Your Efforts

A balance of people, process, and technology.

1. **Know What You Have** – Keep an inventory of what assets you have and where they live.
2. **Manage It Well** – Keep your support contracts active. Apply patches when vendors release them.
3. **Manage Access (and multifactor authentication (MFA))** – Limit who has access to your systems (especially critical or sensitive platforms). If you are compromised or phished, limit the exposure.
4. **Manage Data** – Know where your data is and ensure you're comfortable with those systems' methods of protection. Utilize encryption at rest and in transit.
5. **Build the Right Visibility** – Now that you know where your data is, do you have logs and records of who logged in and accessed it? Collect the data and ensure it is reviewed regularly.
6. **Manage Your Vendors** – Where vendors store or access your data, ensure you are performing due diligence on their security program. Sample questions to consider: Do they adhere to their compliance requirements? Do they have a security program that you are comfortable with? Do they share third party audit reports (e.g. SOC2/SSAE16)?
7. **Empower Your Staff** – Develop a policy & require acceptance. Communicate it and provide basic education. If possible, invest in a security awareness program.



“Companies spend millions of dollars on firewalls and secure access devices...none of these measures address the weakest link in the security chain: the people.”

—Kevin Mitnick, famous hacker

77

206. But Blackbaud’s customers, alone, could not ward off cyberattacks, and Blackbaud knew that a significant amount of the risk fell upon Blackbaud. Blackbaud anticipated that, even if it followed best practices, it could still be the subject of a data breach. Accordingly, Blackbaud

---

<sup>77</sup> *Id.*



developed an Incident Management and Response plan, and provided an overview to its customers.<sup>78</sup>

207. In its Incident Management and Response Overview, Blackbaud noted that its chief concerns in the event of any data breach were to mitigate the impact and duration of a breach. In order to do so, preparation was key:

The objective of Blackbaud's Cyber Security Incident Response program is to promptly and effectively mitigate the **impact** and **duration** of a security relevant incident. In order to accomplish this, we believe much of the hard work occurs long before an incident is ever identified – proper **preparation**. We regularly test the incident response plan via regular table-top exercises used to simulate potential attacks and response scenarios. This facilitates regular practice and continuously improves the incident response function. We also perform regular penetration testing to evaluate our preventative, detective, and responsive security capabilities.

79

208. Blackbaud's Incident Management and Response Overview focuses on the early identification of threats, notification “in a time frame that adheres to the latest compliance standards,” using security infrastructure in place to contain the threat, eradicating any of the tools or applications that a hacker used, restoring access to accounts, and performing “after-action” review to improve systems through detailed security analysis of the incident response.<sup>80</sup>

---

<sup>78</sup> Blackbaud Cyber Security, *Incident Management and Response Overview* (Feb. 2020), [https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/blackbaud\\_incident-management-and-response-overview.pdf?sfvrsn=15d418c6\\_0](https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/blackbaud_incident-management-and-response-overview.pdf?sfvrsn=15d418c6_0).

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

Blackbaud’s practices do not include paying a ransom to mitigate damages associated with a data breach.

209. Blackbaud was also aware of the risk that data breaches would pose by virtue of its understood obligations under foreign law. Blackbaud’s Privacy Shield Notice commits to maintaining “reasonable administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction.”<sup>81</sup> The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are voluntary programs in which U.S. organizations may self-certify that they employ high data protection and security standards. The FTC enforces the Privacy Shield standards and encourages companies to “review their privacy policies to ensure they describe their privacy practices accurately.”<sup>82</sup>

210. Organizations that self-certify under the Privacy Shield Framework must “[d]evelop a Privacy Shield-[c]ompliant [p]rivacy [p]olicy [s]tatement”<sup>83</sup> that, among other things, must “inform individuals about . . . the types of personal data collected.”<sup>84</sup>

211. Blackbaud has self-certified to the Privacy Shield Framework, effective between August 1, 2016 and October 20, 2020.<sup>85</sup> Blackbaud’s Privacy Shield Policy, submitted to the U.S.

---

<sup>81</sup> *Blackbaud Privacy Shield Certification Notice*, Blackbaud (Jan. 1, 2017), [https://fundraising.blackbaud.co.uk/2017/01/01/blackbaud-privacy-shield-certification-notice/?\\_ga=2.190806440.2072851594.1616543868-605719626.1616543868](https://fundraising.blackbaud.co.uk/2017/01/01/blackbaud-privacy-shield-certification-notice/?_ga=2.190806440.2072851594.1616543868-605719626.1616543868).

<sup>82</sup> *Update on the Privacy Shield Framework*, FTC (updated July 21, 2020), <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield>.

<sup>83</sup> *The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks* at 2, Int’l Trade Admin. <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000000QJdg> (last visited Mar. 24, 2021).

<sup>84</sup> *1. Notice*, Privacy Shield Framework, <https://www.privacyshield.gov/article?id=1-NOTICE> (last visited Mar. 24, 2021).

<sup>85</sup> *Other Covered Entities*, Privacy Shield Framework, <https://www.privacyshield.gov/participant?id=a2zt0000000015lAAA> (last visited Mar. 10, 2021).

Department of Commerce and posted publicly on its website became effective August 1, 2016, and was last revised September 18, 2019.<sup>86</sup>

212. Blackbaud's Privacy Shield Notice also contains inaccuracies and unfair misrepresentations. Blackbaud's Privacy Shield Notice purportedly applies to Personal Data as follows:

For purposes of this Notice, "Personal Data" means information that (i) is transferred from the EEA or Switzerland to the United States, (ii) is recorded in any form, (iii) is about, or relates to, an identified or identifiable job applicant, consumer, customer, supplier or other individual (excluding Blackbaud employees), and (iv) can be linked to that job applicant, consumer, customer supplier or other individual.<sup>87</sup>

213. Blackbaud's Privacy Shield Notice commits to maintaining "reasonable administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction."<sup>88</sup>

214. Despite this commitment, Blackbaud did not protect Personal Data from unauthorized access during the Data Breach.

215. Further in its Privacy Shield Notice, Blackbaud states:

216. We do not collect sensitive Personal Data of consumers, customers or suppliers, such as information about medical or health conditions...political opinions, religious or philosophical beliefs...or other sensitive information as defined by the Privacy Shield framework.<sup>89</sup>

---

<sup>86</sup> *Id.*

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

217. This statement is misleading and untrue. Blackbaud markets its “Grateful Patient Programs” (“GPPs”), which collects sensitive information, including medical and health conditions, as well as its other “purpose-built patient engagement solutions”<sup>90</sup> to U.K. and European healthcare organizations, including, inter alia, Operation Smile Ireland, Sarcoma UK, and St Columba’s Hospice.<sup>91</sup>

218. Blackbaud knew of the attendant risks that it and its customers faced as a result of hosting the Private Information of millions of individuals and determined that it, in the regular course of business, developing a robust cybersecurity program, including policies and building upon cybersecurity infrastructure were the best ways to prevent and recover from data breaches.

219. Because of the highly-sensitive and personal nature of Plaintiffs’ Private Information that Blackbaud collects and warehouses, Blackbaud has publicly affirmed its obligation and duty to secure Private Information.

#### **B. Blackbaud’s Responsibility to Safeguard Information**

220. Beyond the obligations created in its security and privacy policies, Blackbaud owed Plaintiffs and class members a duty to safeguard their Private Information.

221. First, as described further below, Blackbaud owed a duty to safeguard Private Information pursuant to a number of statutes, including the HIPAA, the Federal Trade Commission Act (“FTC Act”), Children’s Online Privacy Protection Act (“COPPA”), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and the class members from the type of conduct by Blackbaud alleged herein.

---

<sup>90</sup> *Healthcare Organizations*, Blackbaud, <https://www.blackbaud.co.uk/who-we-serve/healthcare-organisations> (last visited Mar. 24, 2021).

<sup>91</sup> *Customer Stories*, Blackbaud, <https://www.blackbaud.co.uk/customer-stories> (last visited Mar. 24, 2021).

222. Next, Blackbaud owed a duty to safeguard Private Information given that it was on notice that it was maintaining highly-valuable data, for which Blackbaud knew there was a risk that it would be targeted by cybercriminals. Blackbaud knew of the extensive harm that would occur if Plaintiffs' and class members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

223. Given the sensitive nature of the Private Information obtained by the Social Good Entities, Blackbaud knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud if it were able to exfiltrate that data from Blackbaud's servers. Blackbaud also knew that individuals whose Private Information was stored on Blackbaud's servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

224. Blackbaud also owed a duty to safeguard Plaintiffs' and class members' data based upon the promises that it made to its customers to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. Blackbaud voluntarily undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and class members to keep their Private Information secure.

225. Blackbaud also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—it did not do.

**C. Blackbaud Failed to Meet Its Obligations to Protect Private Information or Comply with its own Privacy Policies**

226. Blackbaud's services are supported by privacy policies and security practices, which it provides on a publicly-facing website.

227. Blackbaud was keenly aware of the obligations that state and federal law imposed upon it given the types of information that Blackbaud stored and processed for Social Good Entities.<sup>92</sup>

228. Blackbaud also had a special relationship with Plaintiffs and class members from being entrusted with their Private Information, which provided an independent duty of care. Blackbaud had a duty to use reasonable security measures because it undertook to collect, store and use consumers' Private Information. Regardless of whether an individual entered their information through Blackbaud's website (such as on a hosted form for a charitable entity), or the information was provided to Blackbaud by a Social Good Entity as part of a servicing agreement, Blackbaud owed a duty to protect and safeguard that Private Information. Blackbaud's contention in a recent SEC filing that "plaintiffs lack contractual privity with us"<sup>93</sup> misses the point.

229. Blackbaud has further failed Plaintiffs and class members by its failure to maintain a comprehensive and sufficient security program, including by not adequately securing and protecting Private Information that was stored on outdated legacy tables or files stored on Blackbaud's systems that no longer had a reasonable or practicable business purpose, which, as proven by the Data Breach, were exposed and vulnerable to hacking and theft.

230. Blackbaud failed to provide Plaintiffs and Class Members with timely and adequate notice of the extent of the Data Breach by falsely assuring them in its public statements and Notices issued prior to September 29, 2020, that the attack only impacted certain Private Information and specifically did not include SSNs. Timely notification of the breach was required so that, among

---

<sup>92</sup> Blackbaud Security (Mar. 2, 2020), *available at* <https://web.archive.org/web/20200302212750/https://www.blackbaud.com/security>.

<sup>93</sup> Blackbaud, Inc., Form 10-Q at 20 (Nov. 3, 2020), <https://investor.blackbaud.com/static-files/b861e404-fa85-4f5b-a833-bc30de0165dd>.

other things, Plaintiffs and Class members could take measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to try to prevent identify theft.

231. Remarkably, Blackbaud President and CEO, Mike Gianoni, told The NonProfit Times that Blackbaud had “no reason to believe it [the Data Breach] will result in any public disclosure of any of our customers’ data.”<sup>94</sup>

232. The duty to protect Plaintiffs’ Private Information is non-delegable, particularly here where Blackbaud’s entire business model is premised upon voluntarily assuming the duty by soliciting customers to utilize its professed ability to manage, house, and safeguard data. Accordingly, Blackbaud is liable to Plaintiffs and the Class for the compromise and unauthorized disclosure of their Private Information.

#### **D. Blackbaud Failed to Comply with Industry and Regulatory Standards**

233. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining and securing Private Information, such as Blackbaud, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and

---

<sup>94</sup> See *supra* n.13.

protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.<sup>95</sup> Indeed, Blackbaud recognizes these best practices, and discusses many of them in its security and privacy protocols and policies.

234. Additionally, part of a company's cybersecurity hygiene concerns the ability to patch software and ensure that older databases and servers remain secure. According to Confidential Witness No. 1, the databases that were impacted by the Data Breach were older, and "one of the last vestiges" of Blackbaud's old data center.

235. Further, Federal and State governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.<sup>96</sup>

236. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.<sup>97</sup> The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.<sup>98</sup> The guidelines also

---

<sup>95</sup> See *White Paper: Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), <https://insights.datamark.net/addressing-bpo-information-security/>.

<sup>96</sup> *Start with Security: A Guide for Business* at 2, FTC (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

<sup>97</sup> *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

<sup>98</sup> See *id.*



recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>99</sup>

237. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

238. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

239. Blackbaud also has obligations created by other federal and state law and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and class members' Private Information confidential and to protect it from unauthorized access and disclosure.

240. Blackbaud was no stranger to following stringent security and privacy policies. Upon information and belief, as a government contractor for, inter alia, the Department of the Army, the Department of State, the Department of Veterans Affairs, and the Smithsonian

---

<sup>99</sup> *Id.*

Institution, Blackbaud is subject to cyber security obligations stemming from federal law, such as the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, and 48 C.F.R. § 52.204-21.100

241. Blackbaud also had a duty to safeguard Plaintiffs’ and class members’ PHI under HIPAA and its implementing regulations, 45 C.F.R. §§ 160, et seq., which establish privacy and security standards for certain health organizations and their “business associates.” See *id.* § 164.302. Blackbaud is a “business associate” subject to HIPAA because it receives, maintains, or transmits its customers’ PHI. *Id.* § 160.103. “PHI” includes, in relevant part, individually identifiable health information relating to the provision of health care, such as Plaintiff Clayton’s compromised medical data. *Id.*

242. For example, HIPAA required Blackbaud to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id.* § 160.306(a). To do so, Blackbaud was required to implement reasonable and appropriate security measures to mitigate the risk of unauthorized access to its customers’ electronic personal health information, including by encrypting certain data where appropriate. See *id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

243. Blackbaud similarly violated other statutes by failing to implement reasonable security measures to mitigate the risk of unauthorized access, and encrypting necessary information.

244. Given the magnitude of the risk and repercussions of a breach or attack targeting this type of data, the likelihood of a breach or attack, and Blackbaud’s explicit awareness of these vulnerabilities, Blackbaud should have taken every reasonable precaution in developing a robust

---

<sup>100</sup> Darren Death, *Information Security Requirements for U.S. Federal Contractors*, *Forbes* (Sept. 4, 2018), <https://www.forbes.com/sites/forbestechcouncil/2018/09/04/information-security-requirements-for-u-s-federal-contractors/#4c0c6b83451b>.

security program and protecting Plaintiffs' and the class members' Private Information. However, Blackbaud failed to even employ "appropriate" safeguards as it pledged in its Privacy Policy, leaving the sensitive Private Information in its possession exposed to unauthorized access. This is especially concerning since Blackbaud serves many non-profit organizations, which depend on donor contributions such as those of Plaintiffs to fund their operations, and ultimately allowed the donors' data to be compromised and misused.

245. Despite its duties, representations, and promises, Blackbaud failed to adequately secure and protect its clients' data, including that of the numerous non-profits, such as the respective organizations which maintained Plaintiffs' and the class members' Private Information, allowing the Private Information to be accessed, disclosed, and misused.

**E. Blackbaud's Failures Resulted in a Data Breach**

246. Prior to the ransomware attack and Data Breach, Plaintiffs and class members provided sensitive and personally identifying Private Information to Blackbaud as part of their participation in fundraising by non-profit companies, seeking healthcare from healthcare providers, seeking education from K-12 school providers and universities, and/or seeking other services from Blackbaud's clients, the Social Good Entities. When providing such information, Plaintiffs and class members reasonably expected that the manager and securer of their Private Information, Blackbaud, would maintain security against cybercriminals and cyberattacks.

247. Blackbaud maintained Plaintiffs' and the class members' data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care providers, schools, and other facilities over the course of recent years, Blackbaud did not maintain adequate security of Plaintiffs' and the class members' Private Information, and did not adequately protect it against hackers and cyberattacks.

248. Blackbaud maintained Private Information on servers that were obsolete. According to Confidential Witness No. 1, the servers were not on the system patch schedule and were “forgotten machines.”

249. According to Confidential Witness No. 1, Blackbaud had planned on upgrading the old servers to new technology. The servers that were breached were one of the last environments to be rolled over onto a new platform that Blackbaud was implementing called “Raiser’s Edge.” The older servers, according to Confidential Witness No. 1, were operating multiple applications, and Blackbaud wanted to eventually merge them onto a new, base application on one server. According to Confidential Witness No. 1, upgrading to new technology had been “on a laundry list for a while.”

250. According to Confidential Witness No. 1, employees at Blackbaud became increasingly alarmed with Blackbaud’s failure to patch old systems, and even eventually emailed executives about the vulnerabilities—receiving a response from one executive: “we’re working on it.”

251. Confidential Witness No. 1 also warned Blackbaud about process vulnerabilities that would subject them to attack—such as using remote desktop access and the vulnerabilities that had been uncovered in security scans. According to Confidential Witness No. 1, the remote desktop access configuration was particularly concerning for a year leading up to the data breach—so much so that s/he or his/her team member would simply “shut down the machines” because they knew the risk was too high to allow them to continue to operate.

252. In addition to the emails that Confidential Witness No. 1 and his team sent to executives, prior to the breach s/he separately advised that CrowdStrike needed to be installed on Blackbaud’s machines to capture logs, including the logs that were later erased by the ransomware

in this case. Because Blackbaud elected not to install a program on their servers that would have assisted in the forensic investigation of the Data Breach, the data that would normally be used in a forensic investigation is limited. To be clear: Blackbaud elected to not have this functionality and, as a result, the data on the Data Breach is limited.

253. The ransomware attack that began in February 2020 and continued until May 2020, led to the removal of one or more copies of some or all of the accessed data. Once removed, the hackers could easily have re-copied the stolen data.<sup>101</sup> The ransomware attack was twofold: the cybercriminals copied data from the systems and held it for ransom, and upon being discovered, the cybercriminals attempted but allegedly failed to block Blackbaud from accessing its own systems.<sup>102</sup>

254. The first paragraph of Blackbaud's notice about the Data Breach on its website dated July 16, 2020 (the "Website Notice"), does not inform class members about the true nature of the sensitive Private Information exfiltrated by the hackers; rather, it seeks to normalize hacking and paint Blackbaud as both a victim and a hero, stating:

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. Like many in our industry, Blackbaud encounters millions of attacks each month, and our expert Cybersecurity team successfully defends against those attacks while constantly studying the landscape to stay ahead of this sophisticated criminal industry. We wanted to notify our customers and other stakeholders about a particular security incident that recently occurred.<sup>103</sup>

---

<sup>101</sup> Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, ConsumerAffairs, <https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html> (last visited Mar. 29, 2021).

<sup>102</sup> See *supra* n.3.

<sup>103</sup> *Id.*

255. In fact, Blackbaud’s Website Notice devotes only three of 20 sentences to describing the impact the Data Breach might have on its class members, withholding critical details from the public that would have allowed Plaintiffs and class members to assess the risks to their Private Information and take targeted, but reasonable, precautionary protective measures based on the nature of the incident.

256. Blackbaud stated in its Website Notice that it initially discovered a ransomware attack in May of 2020<sup>104</sup> that attempted to “disrupt the business by locking companies out of their own data and servers.”<sup>105</sup> According to Blackbaud’s statement:

After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. **The cybercriminal did not access credit card information, bank account information, or social security numbers.** Because protecting our customers’ data is our top priority, we paid the cybercriminal’s demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. . . . The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.<sup>106</sup>

257. Overall, Blackbaud’s Website Notice raised more questions about the impact to class members than it answered. For example, Blackbaud’s Website Notice did not:

---

<sup>104</sup> *Security Incident*, Blackbaud (July 19, 2020), <https://www.blackbaud.com/securityincident> [<https://web.archive.org/web/20200719170537/https://www.blackbaud.com/securityincident>].

<sup>105</sup> *Id.*

<sup>106</sup> *Id.* (emphasis added). Notably, the language in bold has since been removed. *See Security Incident*, Blackbaud (updated Sept. 29, 2020), <https://www.blackbaud.com/securityincident> (last visited Mar. 18, 2021).

- a. disclose the size of the Data Breach (an unspecified “subset” of individuals were impacted);
- b. explain why Blackbaud waited approximately two months to notify authorities of the Data Breach after the ransomware attack was detected;
- c. explain how the hackers gained access to Blackbaud’s system (*e.g.*, via phishing or an exploit kit);
- d. explain the nature of the “confirmation” that the copy of the data the cybercriminals removed “had been destroyed;”
- e. explain what specific facts cause Blackbaud to believe that the exfiltrated data will not be misused by the individuals who stole it, despite those individuals having already proven to be criminal by their actions;
- f. explain what specific changes Blackbaud “implemented . . . to prevent this specific issue from happening again” or what vulnerabilities the attack exposed that needed to be remediated; or
- g. say whether the method is used to “prevent[] the cybercriminal from blocking our system access and fully encrypting [our] files” was actually the payment of a ransom to the cybercriminals.<sup>107</sup>

258. Blackbaud’s opaque data breach announcement has left Plaintiffs and class members with more questions than answers. Blackbaud’s lack of transparency means that Plaintiffs and class members still do not know how Blackbaud restricted access to Private Information or the extent to which it practiced cybersecurity hygiene, such as data minimization or deleting data after a certain period of time. Similarly, Blackbaud has completely failed to provide basic information about the Data Breach, itself, to the public—including when it was actually first detected; what Private Information was compromised, accessed, and exfiltrated; which security and privacy practices were insufficient (or not followed) so as to allow the Data Breach to occur; what Blackbaud is doing to prevent future data breaches; what representations were made by the cybercriminals during the ransom negotiations; and how can Blackbaud be assured that the cybercriminals will not target the individuals whose Private Information was taken.

---

<sup>107</sup> *Id.*; *supra* n.3.

259. Blackbaud's lack of clarity about the extent of the information that was comprised, has left Plaintiffs and class members to fend for themselves, spending time, effort, and money to protect themselves in the wake of the Data Breach.

260. Both the Security Incident and blog pages on Blackbaud's website are devoid of any explanation to the affected individuals as to how they could protect themselves with credit freezes, credit monitoring, or other action.

261. Although Blackbaud originally claimed in its Website Notice that credit card information and bank account information was not accessed, from August 17, 2020 through September 3, 2020, many Social Good Entities warned individuals that their sensitive data, including SSNs and payment information, may actually have been accessed.<sup>108</sup>

262. Plaintiffs received notices advising individuals whose Private Information was accessed to, inter alia, "remain vigilant over the next twelve to twenty-four months for any strange inquiries, including potential phishing attempts," and report "any suspicious activity or suspected identity theft." Furthermore, one Notice furnished to Plaintiff Case advised that the organization "cannot be completely certain" that Blackbaud was indeed able to retrieve the stolen data. In at least one other notice, the institution advised that it was "examining our vendor relationship with Blackbaud and evaluating their security safeguards."

---

<sup>108</sup> See, e.g., Notice Letter from University of Detroit Mercy, <https://oag.ca.gov/system/files/9028629.PDF> (warning that cybercriminals may have accessed individuals' full name and SSN); bigthought.org, *Blackbaud Security Breach and How it Affects You, Your Privacy, and Big Thought*, <https://www.bigthought.org/announcements/news-announcements/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought/> (last visited Mar. 29, 2021) ("Although Blackbaud has stated that all information was encrypted, a social security number or employment identification number (EIN) may have been accessible to the cybercriminal..."); HIPAA Journal, *56,000 Northwestern Memorial HealthCare Donors Impacted by Blackbaud Ransomware Attack*, <https://www.hipaajournal.com/56000-northwestern-memorial-healthcare-donors-impacted-by-blackbaud-ransomware-attack/> (last visited Mar. 29, 2021) (noting that the database contained the SSNs and/or financial payment card information of individuals).



263. Blackbaud originally (and falsely) reported that no SSNs, bank account information, or other financial data was compromised. For example, Plaintiff Glasper received a notice from Allina Health informing him that the information that could have been accessed “DID NOT include: [c]redit card information, [b]ank account information, Social [S]ecurity numbers, [and] [a]ny additional medical information, such as diagnosis or treatment plan.”

264. Blackbaud’s defective notice further increased the likelihood of harm to Plaintiffs and class members by suggesting that the Social Good Entities were “unlikely” to have data breach notification obligations to their students, patients, constituents, and donors.<sup>109</sup> This improper suggestion may have caused some Social Good Entities to delay notifying class members and some to never be notified at all.

265. As a result of Blackbaud’s lax data protection standards, cybercriminals obtained access not only to recently-obtained information, but Private Information that remained on backup files for years, if not decades. For example, one Notice warned “we cannot determine with certainty that the [i]nformation will not be misused.” This Notice also advised that “[u]nfortunately, the cybercriminal removed a copy of the backup files of many of its customers, including our backup file that may have contained your personal information.”

266. Moreover, Blackbaud’s initial assurances that SSNs and other sensitive data had not been accessed ultimately proved false. As late as September 14, 2020, as reflected in a letter from an attorney representing not-for-profit Lakes & Prairies Community Action Partnership, Blackbaud had provided assurances that SSNs and other “sensitive text fields” on Blackbaud’s

---

<sup>109</sup> Letter from Anjali Das, attorney at Wilson Elser Moskowitz Edelman & Dicker LLP, to Wayne Stenehjem, North Dakota Attorney General, at PDF p. 5 (Sept. 14, 2020), <https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2020-09-14-LakesPrairiesCAP.PDF>.

Financial Edge platforms, even in back-up data, were encrypted. However, in September and October 2020, Blackbaud informed certain of its customers that, in fact, such information had been compromised—and, shockingly, this breach occurred in some instances because Blackbaud had maintained much of this sensitive Private Information for decades without encryption, making it particularly vulnerable to theft. Plaintiff Roth received a Notice from his children’s former school that stated “Blackbaud indicated that certain information previously believed to have been encrypted was subsequently determined . . . to not have been encrypted, and that the compromised file may have contained your full name, Social Security number, date of birth, and address.”

267. The Data Breach was the result of Blackbaud’s failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove old unused and obsolete data containing Private Information or to encrypt such information. Blackbaud, in fact, had no valid business reason for retaining such records containing highly sensitive Private Information—including SSNs—for such long periods and for failing to delete or encrypt such information. For example, the letter from Blackbaud to one of its educational institution customers impacted by the Data Breach stated that SSNs of former students and their parents, as well as faculty members, were exposed on unused tables in a legacy version on Blackbaud’s systems.

268. Remarkably, Blackbaud’s retention of this Private Information in unencrypted form on older legacy versions of its programs made public exposure of such data in a cyberattack very likely. It is particularly egregious that Blackbaud continued to keep legacy versions of the software on its systems, despite the fact that, by the time of the Data Breach, there was no valid business reason to continue to maintain this information on its systems. The failure was knowing, reckless and, at bare minimum, negligent given the known risks to Blackbaud—particularly given vendor

announcements regarding the sunset of certain databases and Blackbaud's failure to move Private Information to newer systems with more robust security features. The breach of Plaintiffs and class members' Private Information, particularly their SSNs, is a direct consequence of this conduct.

269. Accordingly, Blackbaud's statements of reassurance were unfounded, particularly in light of Blackbaud's earlier admission to the SEC that: "further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords."<sup>110</sup>

270. Blackbaud did not have a sufficient security program in place to prevent cyberattack and access, which is evident by its own statements after the Data Breach that it has "already implemented changes to prevent this specific issue from happening again."<sup>111</sup>

271. Blackbaud's reliance on the word of cybercriminals or a "certificate of destruction" issued by those same thieves that the "copied" or stolen subset of any data was destroyed is patently unreasonable. Blackbaud has not and cannot be assured that SSNs, bank account numbers, and credit card numbers were not also accessed and retained by the cybercriminals, particularly insofar as it advised its clients to inform affected individuals to monitor accounts for suspicious activity and/or identity theft. Despite recognizing the need for ongoing monitoring due to significant heightened risk, Blackbaud has offered no remuneration in the event of actual identity theft or misuse.

272. Likewise, reputable third parties have questioned the reasonableness of Blackbaud's faith in the cybercriminals and encouraged those individuals impacted by the Data

---

<sup>110</sup> Form 8-K, *supra* n.25, at 2.

<sup>111</sup> *Supra* n.3.

Breach to take measures to protect against targeted future criminal activity.<sup>112</sup> For example, the Michigan Attorney General's office rejected Blackbaud's reliance on the promises of cybercriminals, noting that "Blackbaud claims that it has 'no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly' but, to date, has not announced any concrete substantiation of this claim."<sup>113</sup>

273. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, stating that it "does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data."<sup>114</sup> Several media outlets and industry groups have likewise questioned reliance on promises by cybercriminals.<sup>115</sup> Additionally, many Social Good Entities' own Data Breach notices rightly advise affected individuals to monitor their own credit and financial accounts for suspicious account activity and notify the Social Good Entity of any such activity.<sup>116</sup>

---

<sup>112</sup> Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), <https://www.bbc.com/news/technology-53567699> ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.").

<sup>113</sup> Phishing Scams Following Blackbaud Security Breach, Michigan Dep't Attorney General, [https://www.michigan.gov/ag/0,4534,7-359-81903\\_20942-540014--,00.html](https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html) (last visited Mar. 18, 2021).

<sup>114</sup> *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), <https://www.ic3.gov/Media/Y2019/PSA191002>.

<sup>115</sup> See, e.g., Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), <https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/>; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TechCrunch (Oct. 7, 2020), <https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/>.

<sup>116</sup> Letter from Jeffrey Boogay, attorney at Mullen Coughlin LLC, to Consumer Protection Bureau, Office of the New Hampshire Attorney General (Aug. 21, 2020),

274. Thus, despite Blackbaud's claim to the contrary, Blackbaud cannot reasonably rely on the promises of cybercriminals that they destroyed the exfiltrated data after Blackbaud paid those cybercriminals a ransom. Even now, because of its insistence on this illogical reliance, Blackbaud knowingly and recklessly continues to mislead Plaintiffs and class members regarding the scope and potential impact of the Data Breach.

275. Despite having knowledge of the attack and compromised stolen data since at least May 2020, Blackbaud willfully and knowingly withheld this knowledge from its affected clients and their constituents who were victims of the fraud until mid-July or August 2020.

276. Blackbaud has obligations and duties created by state and federal law, contracts, industry standards, common law, and representations made to the clients who entrusted Plaintiffs' and others' data to Blackbaud's care to keep Private Information secure, confidential, and protected from unauthorized access and disclosure.

277. Indeed, cyberattacks have become so notorious that, as recently as November 2019, the FBI and the U.S. Secret Service issued warnings to potential targets like Blackbaud, so they are aware of and are prepared for a potential attack.<sup>117</sup>

278. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Blackbaud's industry, including by Blackbaud's own admissions in its 2019 Annual Report.<sup>118</sup>

---

<https://www.doj.nh.gov/consumer/security-breaches/documents/heifer-project-international-20200901.pdf> (last visited Mar. 10, 2021); Letter from University of Detroit Mercy regarding Notice of Data Breach, <https://oag.ca.gov/system/files/9028629.PDF> (last visited Mar. 18, 2021).

<sup>117</sup> Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), <https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Mar. 10, 2021) (emphasis added).

<sup>118</sup> 2019 Form 10-K, *supra* n.8, at 20.

279. Blackbaud breached its obligations to Plaintiffs and the class members, and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Blackbaud's computer systems and data. Blackbaud's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security program to reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect consumers' Private Information;
- c. Failing to properly monitor its own data security programs for existing intrusions;
- d. Failing to destroy highly confidential personal data information including Social Security numbers on its legacy software which was unnecessarily kept on Blackbaud's systems despite no reasonable or practicable business reason for doing so; and
- e. Failing to timely notify its Clients, Plaintiffs, and the class members of the data breach.

280. As the result of Blackbaud's failure to take certain measures to prevent the attack before it occurred, Blackbaud negligently and unlawfully failed to safeguard Plaintiffs' and class members' Private Information.

281. Accordingly, as outlined below, Plaintiffs' daily lives were disrupted; Plaintiffs and class members experienced actual incidents of identity theft and fraud, and Plaintiffs and class members face an increased risk of fraud and identity theft.

**F. Data Breaches Put Consumers at Increased Risk of Fraud and Identify Theft**

282. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of \$182.5

billion and net income of \$40.2 billion.<sup>119</sup> \$160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about the users of its various free products and services. America's largest corporations profit almost exclusively through the use of Private Information illustrating the considerable market value of personal Private Information.

283. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

284. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

285. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a

---

<sup>119</sup> Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), <https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm>.

Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

286. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

287. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"<sup>120</sup> An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

288. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."<sup>121</sup>

---

<sup>120</sup> Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ>.

<sup>121</sup> *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), <https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks>.



289. The FBI concurs, listing “applying two-factor authentication wherever possible” as a best practice to defend against ransomware attacks.<sup>122</sup>

290. The industries that Blackbaud serves have seen a substantial increase in cyberattacks and data breaches since as early as 2016.<sup>123</sup>

291. Indeed, cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.<sup>124</sup>

292. Cyberattacks and data breaches of medical facilities, educational and religious institutions, and non-profit entities are especially problematic because of the disruption they cause to the daily lives of the patients, students, donors, and other individuals affected by attack, including minor children and adults lacking capacity to consent to the disclosure of their information.

293. Perhaps most illustrative of the danger that can be caused by cyberattacks on medical facilities, the first known death from a cyberattack was recently reported in Germany after a ransomware attack crippled a hospital’s systems and they were forced to turn away emergency patients.<sup>125</sup>

---

<sup>122</sup> *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), <https://www.ic3.gov/Media/Y2016/PSA160915>.

<sup>123</sup> *Id.*

<sup>124</sup> Kochman, *supra* n.117.

<sup>125</sup> Melissa Eddy & Nicole Perlroth, *Cyber Attack Suspected in German Woman’s Death*, N.Y. Times (Sept. 18, 2020), <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html>.

294. The U.S. Government Accountability Office (“GAO”) released a report in 2007 regarding data breaches finding that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>126</sup>

295. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>127</sup>

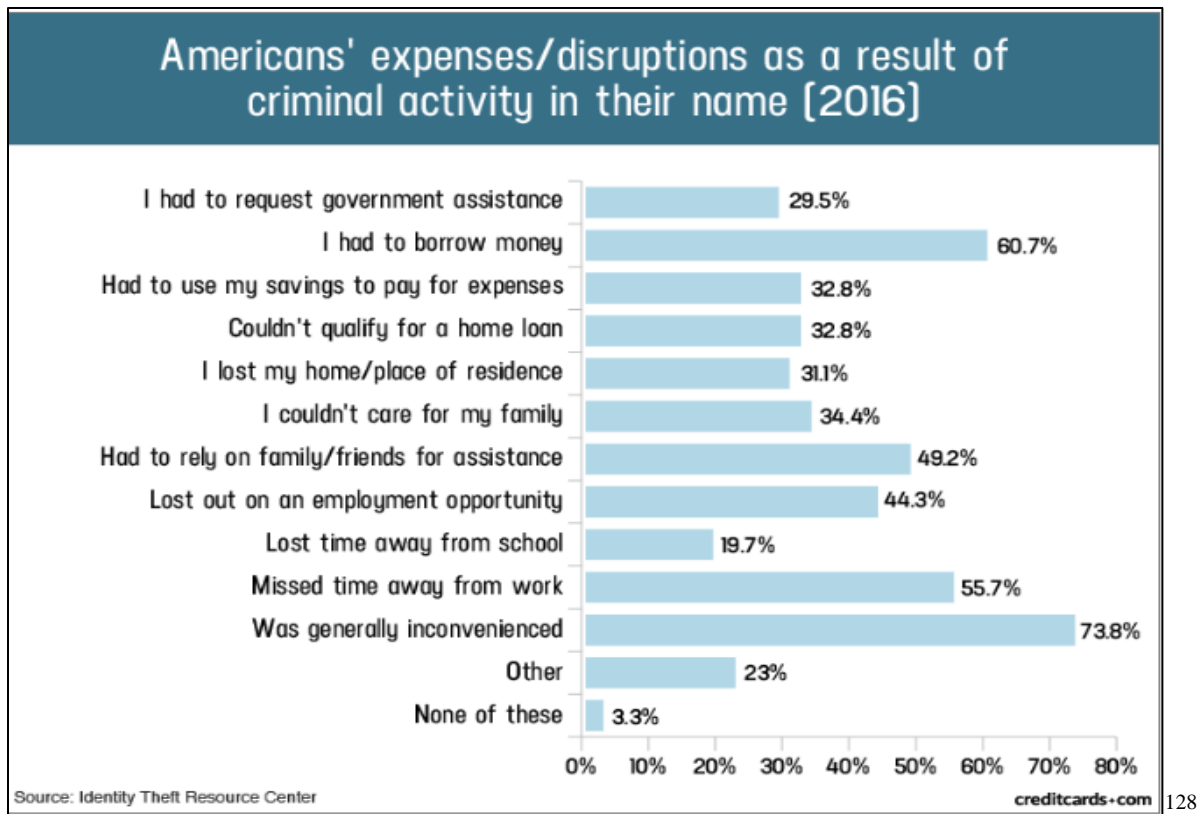
296. Cybercriminals use stolen Private Information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

297. Identity thieves can also use SSNs to obtain a driver’s license or other official identification card in the victim’s name, but with the thief’s picture; use the victim’s name and SSN to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s SSN, rent a house or receive medical services in the victim’s name, seek unemployment or other benefits, and may even give the victim’s Private Information to police during an arrest resulting in an arrest warrant being issued in the victim’s name. A study by the Identity Theft Resource Center (“ITRC”) shows the multitude of harms caused by fraudulent use of personal and financial information:

---

<sup>126</sup> *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (“GAO Report”) at 2, GAO (June 2007), <https://www.gao.gov/assets/270/262899.pdf>.

<sup>127</sup> *Identity Theft Recovery Steps*, FTC, <https://www.identitytheft.gov/Steps> (last visited Mar. 23, 2021).



298. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.<sup>129</sup> As illustrated in the above graphic, this includes devastating results such as “I lost my home/place of residence” and “I couldn’t care for my family.” Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.<sup>130</sup> The ITRC

<sup>128</sup> Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

<sup>129</sup> *Id.*

<sup>130</sup> *Id.*

study concludes that “identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual.”<sup>131</sup>

299. Private Information is a valuable property right.<sup>132</sup> Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

300. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>133</sup>

Private Information is such an inherently valuable commodity to identity thieves that, once it compromised, criminals often trade the information on the cyber black-market for years.

301. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase

---

<sup>131</sup> *Id.*

<sup>132</sup> See, *e.g.*, John T. Soma et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at \*1 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”).

<sup>133</sup> GAO Report, *supra* n.126, at 29.

the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.<sup>134</sup>

302. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and the class members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many of the Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Notices advise, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

**G. Blackbaud’s Inadequate Response to the Data Breach**

303. Upon information and belief, to date, Blackbaud has provided only certain class members with “Single Credit Bureau Monitoring,” which provides data access to only one of the three national credit reporting bureaus, as well as “access remediation support” from CyberScout Fraud Investigator, for a period of only 24 months from the date of enrollment. This is plainly inadequate, as the compromised Private Information can be utilized by thieves at any time after two years, and as such the threat to Plaintiffs’ and the class members’ credit or identity will continue for many years thereafter. Beyond this two-year window, Blackbaud offers these victims no assistance or protection, even if identity theft occurs. Consequently, Plaintiffs and class members have and will incur out of pocket costs including the costs of purchasing credit

---

<sup>134</sup> See *supra* n.113 (concluding that personal information such as “names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware”).

monitoring services, credit freezes, credit reports, and/or other protective measures to deter, detect, respond to, and address identity theft.

304. As a result of the Data Breach, even if Plaintiffs used credit monitoring, the data thieves could wait another seven or more years to sell or use their Private Information without detection. Moreover, cybercriminals may be able to cross-reference information obtained from this Data Breach with other data sources with an astonishingly comprehensive scope and degree of accuracy to build valuable profiles on Plaintiffs and members of the class. Two years of single-bureau credit monitoring is not enough to protect against these attacks.

305. Further, even if the class members' credit is frozen, they will eventually need to unfreeze their credit in order to, among other things, obtain any car loans, obtain any mortgages, apply for jobs and various other tasks associated with building and strengthening their credit histories. Doing so will make the class members vulnerable again in the future.

## **VI. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES**

306. Plaintiffs and class members have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May of 2020, Plaintiffs did not receive Notice until July of 2020 at the earliest—*nearly six months after the breach began*.

### **A. Plaintiffs' and Class Members' Private Information was Compromised in the Data Breach**

307. This security incident is not limited to automated attacks against the availability of information in Blackbaud's possession, custody or control. This incident included unauthorized persons taking possession of the information, available for their use however and whenever they see fit.

308. Plaintiffs include students and donors to educational institutions, healthcare patients and donors to healthcare organizations, as well as donors to other non-profit organizations—such as international relief funds, museums, charitable trusts, legal rights organizations, animal welfare organizations, child welfare organizations, as well as national and local charities. Plaintiffs were required to provide Private Information that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard.

309. Like Plaintiffs, the class members' Private Information was compromised as a direct and proximate result of the Data Breach.

310. As a direct and proximate result of Blackbaud's conduct, Plaintiffs and the class members have been damaged because of the disclosure of their Private Information in several ways.

311. First, because Blackbaud paid a ransom to the cybercriminals to avoid disclosure of the data that was already stolen, Blackbaud has already demonstrated to those criminals that the stolen data has value. Accordingly, now Plaintiffs and class members face their own risk of extortion, because there can be no guarantee that the cybercriminals actually deleted the data that they stole.

312. Although Blackbaud will argue that its payment of a ransom diminishes the risk to Plaintiffs and class members to close to zero, privacy and security professionals disagree, and believe that payment of a ransom may encourage further exploits.

Unlike negotiating for a decryption key, *negotiating for the suppression of stolen data has no finite end*. Once a victim receives a decryption key, it can't be taken away and does not degrade with time. With stolen data, a threat actor can return for a second payment at any point in the future. The track records are too short and evidence that defaults are selectively occurring is already collecting. Accordingly, we strongly advise all victims of data exfiltration to take the hard, but responsible steps. Those include getting the advice of competent privacy attorneys, performing an investigation into what data was taken, and performing the necessary

notifications that result from that investigation and counsel. *Paying a threat actor does not discharge any of the above, and given the outcomes that we have recently seen, paying a threat actor not to leak stolen data provides almost no benefit to the victim.*<sup>135</sup>

313. The risk borne by Plaintiffs and class members is a real one, evidenced by the notices received by the Plaintiffs, which continue to advise Plaintiffs to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

314. Second, Plaintiffs and class members have sustained injuries as a result of the disclosure of their Private Information to unauthorized third-party cybercriminals as a result of Blackbaud's insufficient cybersecurity.

315. Plaintiffs have lost the value of their Private Information because the information is a valuable commodity. As discussed herein, Blackbaud demonstrated its value when it paid a ransom to avoid its disclosure. The cybercriminals also recognize its value—placing a price on what it would cost to prevent the disclosure of that information. Further, Blackbaud recognizes the value of the Private Information because it is paid handsomely to protect it.

316. Plaintiffs face real, concrete, and cognizable injuries as a result of the ransomware attack, because cybercriminals confirmed that they exfiltrated data from Blackbaud's systems, and cybersecurity professionals agree that Blackbaud cannot trust the word of criminals in ensuring the safety of Plaintiffs' and class members' Private Information. The payment of a ransom cannot ensure that the data was deleted, and the Social Good Entities have even warned Plaintiffs and class members that they must be diligent to prevent identity theft and fraud from occurring as a result of the Data Breach.

---

<sup>135</sup> *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues, supra* n.41 (emphasis added).



317. As a result, Plaintiffs and class members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

318. Plaintiffs and the class members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs. As a result of Blackbaud's payment of the ransom to the cybercriminals, Blackbaud has also placed Plaintiffs and class members at risk for being targeted to make ransom payments, themselves, to prevent the disclosure and dissemination of the Private Information that was taken from Blackbaud's systems.

319. Further, Blackbaud has not provided sufficient information to allow Plaintiffs and class members to adequately protect themselves. As a direct and proximate result of Blackbaud's conduct, Plaintiffs and the class members have and will continue to incur out-of-pocket costs for protective measures such as on-going credit monitoring fees and may also incur additional costs for credit report fees, and similar costs directly related to the Data Breach.

320. Plaintiffs and the class members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and the class members have and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Addressing their inability to withdraw funds linked to compromised accounts;
- d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- e. Placing "freezes" and "alerts" with credit reporting agencies;

- f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- g. Contacting financial institutions and closing or modifying financial accounts;
- h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;
- j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and
- k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

321. Further, Plaintiffs and class members will have to continue to spend significant amounts of time to respond to the Data Breach and monitor their financial, student, and medical accounts and records for misuse.

322. Third, Plaintiffs have, at the very least, sustained nominal damages for Blackbaud's violations as discussed herein. As a result of Blackbaud's failures to safeguard Plaintiffs' and the class members' Private Information, they are forced to live with the knowledge that their Private Information—which contains private and personal details of their life—may be disclosed to the entire world, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiffs and the class members of their fundamental right to privacy.

323. Fourth, Plaintiffs are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below.

324. Fifth, Blackbaud was unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members. Among other things, Blackbaud continues to benefit and profit from

class members' Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

325. Finally, Plaintiffs and the class members have an interest in ensuring that their Private Information, which remains in the possession of Blackbaud, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiffs' and the class members' data is not accessible online and that access to such data is limited and secured.

**B. The Private Information of Minors Was Also Compromised in the Data Breach**

326. Plaintiffs include guardians of minor students of educational institutions, who were required to provide Private Information that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard. In some instances, this information included the student's academic records as well as sensitive Private Information.

327. Children's data is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity. Specifically:

The theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to go to college and start applying for student loans or get their first credit card. By then, the damage is done and the now young adult will need to go through the pain of proving that their identity was indeed stolen.<sup>136</sup>

---

<sup>136</sup> Avery Wolfe, *How Data Breaches Affect Children*, AXIOM Cyber Solutions (Mar. 15, 2018), <https://axiomcyber.com/data-breach/how-data-breaches-affect-children/>.

328. In 2011, Carnegie Mellon University’s CyLab reported “the rate of child identity theft is 51 times higher than for adults (whose data sets cost about \$10 - \$25 on dark web markets).”<sup>137</sup>

329. By early 2018, it became well known that the data of infants was being sold on the dark web. As of 2018, the cost of an infant’s data was approximately \$300 in Bitcoin, which would “provide cybercriminals access to a clean credit history.”<sup>138</sup>

330. As instructed by the FTC:

A child’s Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live.<sup>139</sup>

331. As one cyber-security author further explained, the impact of the use of children’s information is further exacerbated by the fact that there are few checks on using a child’s data to initially obtain credit and slowly increase it over time—all while being undetected by the child and the parents.<sup>140</sup> Thus, “[t]he problem goes unnoticed for years—possibly decades—before the child goes to apply for student loans, open their first credit card, or buy their first car.”<sup>141</sup>

---

<sup>137</sup> Selena Larson, *Infant Social Security Numbers Are for Sale on the Dark Web*, CNN Bus. (Jan. 22, 2018), <https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html>.

<sup>138</sup> *Id.*

<sup>139</sup> *Child Identity Theft*, FTC: Consumer Info. (Sept. 2018), <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.

<sup>140</sup> See Emily Wilson, *The Worrying Trend of Children’s Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), <https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/>.

<sup>141</sup> *Id.*

332. In light of regulations about how children’s Private Information is collected and maintained, the companies providing the service of collecting and maintaining purport to understand this critical concern about the safe keeping of children’s data.

333. Blackbaud has made specific commitments regarding the maintenance of students’ Private Information. In April of 2015, with regard to its K-12 school providers, Blackbaud signed a pledge to respect student data privacy to safeguard student information. The Student Privacy Pledge (the “Pledge”) was created to “safeguard student privacy in the collection, maintenance and use of personal information.”<sup>142</sup>

334. In signing the Pledge, Blackbaud represented to students and parents of its K-12 school providers that it would, (1) “[m]aintain a comprehensive security program:” and (2) “[b]e transparent about collection and use of student data.”<sup>143</sup> Additionally, “[t]he Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.”<sup>144</sup>

335. In further support of this representation and promise to student and parent users, Travis Warrant, president of Blackbaud’s K-12 Private Schools Group, stated:

Blackbaud is committed to protecting sensitive student data and security . . . . The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy. The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.<sup>145</sup>

---

<sup>142</sup> Nicole McGougan, *Blackbaud Signs Pledge to Respect Student Data Privacy*, Blackbaud (Apr. 22, 2015, 1:11 PM), <https://www.blackbaud.com/newsroom/article/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy> (last visited Mar. 10, 2021).

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*

336. Accordingly, the minors have also suffered concrete and particularized injuries as a result of the Data Breach.

**C. Plaintiffs’ and Class Members’ PHI was Compromised in the Data Breach**

337. Another group of individuals whose Private Information was compromised in the Data Breach include healthcare patients and donors to healthcare organizations, who were required to provide PHI that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard.

338. Hospital and healthcare provider GPPs must comply with HIPAA and the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, including the HHS implementing regulations.

339. A 2013 HIPAA amendment made it easier for HIPAA Covered Entities, such as hospitals and healthcare providers, to target patients for donations by using software solutions like those offered by Blackbaud to enrich electronic Protected Health Information (“ePHI”) to maximize outreach to wealthy patients capable of making a meaningful philanthropic gift to the hospital.

340. ePHI is PHI that is produced, saved, transferred, or received in electronic form. PHI is “[i]ndividually identifiable health information . . . received by a health care provider, health plan, employer or healthcare clearing house [and its Business Associates] . . . [that] [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual . . . [t]hat identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. §§ 160.103, et seq.

341. Under the 2013 HIPAA amendments, Covered Entities such as hospitals are permitted to use and disclose ePHI without a written patient authorization for GPPs, including, without limitation, data elements such as the patient's name, age, gender, date of birth, dates of services, patient's health insurance status, the department treating the patient (e.g., oncology), the name of the patient's physician, and the outcome of the patient's care.

342. Blackbaud provides software solutions to Covered Entities with GPPs.

343. Upon information and belief, Blackbaud's Covered Entity Clients enter ePHI into Blackbaud hosted solutions for purposes including, but not limited to, analyzing the ePHI in combination with publicly available sources to identify major and principle gift prospects.

344. Blackbaud understood and made representations to the Social Good Entities about both the value and the risk of using ePHI for fundraising purposes. As stated in one of its white papers, Blackbaud understood;

[t]he new HIPAA rules offer great opportunity for hospitals and health systems to reach out in a more meaningful way to the individuals and families who have the greatest affinity to them — their patients. **However, with this opportunity comes great responsibility to establish business processes that allow for successful fundraising but also manage and protect the patient data entrusted to you.**<sup>146</sup>

345. Covered Entities and their Business Associates, which process PHI and ePHI, must meet strict privacy and security standards propounded by the U.S. Department of Health and Human Services ("HHS") pursuant to HIPAA and HITECH. HHS's Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules under HIPAA and HITECH.

346. HIPAA/HITECH mandated security specifications are risk-driven and certain measures must be taken if, after a risk assessment, the specified security measure is determined to

---

<sup>146</sup> Susan U. McLaughlin, *HIPAA, PHI, and You*, at 4, Blackbaud (Feb. 2015), [https://www.blackbaud.com/files/resources/downloads/2015/02.15.HIPAA\\_GratefulPatient.Whitepaper.pdf](https://www.blackbaud.com/files/resources/downloads/2015/02.15.HIPAA_GratefulPatient.Whitepaper.pdf) (emphasis added).

be “reasonable and appropriate” in the risk management of the confidentiality, availability, and integrity of ePHI.

347. Encryption of ePHI at rest is a commonly implemented security measure for ePHI stored on systems that can be accessed from the internet (including through a client portal).

348. In fact, HHS mandates that organizations encrypt ePHI in motion and at rest whenever it is “reasonable and appropriate” to do so. If encryption is reasonable and appropriate and an organization fails to implement it, it must document its reasons for not doing so in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

349. Upon information and belief, Blackbaud is a Business Associate, as that term is defined in HIPAA and HITECH, providing functions that involve the use or disclosure of PHI by Covered Entities.

350. In fact, several notices regarding the Data Breach identify Blackbaud as a “Business Associate.”

351. As a Business Associate, Blackbaud is directly subject to the HIPAA Security Rule.

352. As a Business Associate, Blackbaud is directly liable for HIPAA violations for any “failure to comply with the requirements of the Security Rule.”

353. As a Business Associate, Blackbaud is also directly liable for HIPAA violations for any “failure to provide breach notification to a covered entity or another business associate.”

354. The HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the FTC,



apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

355. A HIPAA breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- b. The unauthorized person who used the PHI or to whom the disclosure was made;
- c. Whether the PHI was actually acquired or viewed; and
- d. The extent to which the risk to the PHI has been mitigated.

356. HHS's OCR issued a "Fact Sheet" on "Ransomware and HIPAA."<sup>147</sup> Where there is an unauthorized disclosure or ransomware attack on PHI the Business Associate must document by "thorough and accurate evaluation the evidence acquired and analyzed" to determine whether there is a "low probability of compromise."<sup>148</sup>

357. Blackbaud was aware of the significant privacy and security obligations of Covered Entities and their Business Associates mandated by HIPAA and HITECH and the Privacy and Security Rules.

358. In fact, Blackbaud publishes a white paper on its website describing HIPAA privacy and security issues inherent in the collection and disclosure of PHI for fundraising purposes.<sup>149</sup>

---

<sup>147</sup> *FACT SHEET: Ransomware and HIPAA*, OCR, <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (last visited Mar. 23, 2021).

<sup>148</sup> *Id.* at 6.

<sup>149</sup> *Supra* n.146.

359. Based on the Notices issued by Blackbaud's Covered Entity Clients to their patients, Entities that were using Blackbaud software to enrich ePHI were impacted by the Data Breach.

360. Blackbaud's Covered Entity Clients notified their patients of likely unauthorized exposure of PHI stored by Blackbaud on its servers in an unencrypted manner.

361. Blackbaud also designs products for GPPs, which use applications including but not limited to Blackbaud's Research Point software tool. GPPs are fundraising activities conducted in support of nonprofit hospitals and healthcare providers that allow hospitals to identify major philanthropic gift prospects from their patient populations. As described by *The New York Times*, in furtherance of GPPs:

Many hospitals conduct nightly wealth screenings [of hospital patients] — using software that culls public data such as property records, contributions to political campaigns and other charities — to gauge which patients are most likely to be the source of large donations. Those who seem promising targets for fund-raising may receive a visit from a hospital executive in their rooms, as well as extra amenities like a bathrobe or a nicer waiting area for their families.<sup>150</sup>

362. Through Blackbaud's GPP, hospitals and healthcare systems collect and utilize medical information such as patient numbers, dates of treatment(s), departments of treatment(s), room numbers, health insurance status, and other data that may easily reveal medical diagnosis and related PHI (e.g., being treated by the oncology department would reveal the patient was treated for a cancer diagnosis). This information is collected—without authorization from the patient—and analyzed to determine what kind of donation a former patient would likely make.

---

<sup>150</sup> Phil Galewitz, *Hospitals Are Asking Their Own Patients to Donate Money*, N. Y. Times (Jan. 24, 2019), <https://www.nytimes.com/2019/01/24/business/hospitals-asking-patients-donate-money.html>.

363. Accordingly, Plaintiffs and class members whose PHI was compromised in the Data Breach sustained additional injuries, including statutory damages related to the exposure of their PHI.

## **VII. CLASS ACTION ALLEGATIONS**

364. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as “class members.”

365. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiffs propose the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

**Nationwide Class:** All natural persons residing in the United States whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

366. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose state subclasses as necessary or appropriate.

367. Excluded from the Class and Subclasses are Blackbaud’s officers, directors, and employees; any entity in which Blackbaud has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Blackbaud. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

368. Numerosity under Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous and geographically dispersed that individual joinder of all class members is impracticable. While the exact number of class members is unknown to Plaintiffs at this time, based on information and belief, the class consists of millions of persons whose data was compromised in the Data Breach, who can be identified by reviewing the Private Information exfiltrated from Blackbaud’s databases.

369. Commonality under Federal Rule of Civil Procedure 23(a)(2). There are questions of law and fact common to Plaintiffs and class members, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

- a. Whether Blackbaud unlawfully used, maintained, lost, or disclosed Plaintiffs' and the class members' Private Information;
- b. Whether Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- c. Whether Blackbaud truthfully represented the nature of its security systems, including their vulnerability to hackers;
- d. Whether Blackbaud's data security programs prior to and during the Data Breach complied with applicable data security laws and regulations;
- e. Whether Blackbaud's data security programs prior to and during the Data Breach were consistent with industry standards;
- f. Whether Blackbaud owed a duty to class members to safeguard their Private Information;
- g. Whether Blackbaud breached its duty to class members to safeguard their Private Information;
- h. Whether cyberhackers obtained, sold, copied, stored or released class members' Private Information;
- i. Whether Blackbaud knew or should have known that its data security programs and monitoring processes were deficient;
- j. Whether the class members suffered legally cognizable damages as a result of Blackbaud's misconduct;
- k. Whether Blackbaud's conduct was negligent;
- l. Whether Blackbaud's conduct was negligent *per se*;
- m. Whether Blackbaud's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- n. Whether Blackbaud failed to provide accurate and complete notice of the Data Breach in a timely manner; and
- o. Whether the class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

370. Typicality under Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of those of the class members because Plaintiffs' Private Information, like that of every class member, was compromised in the Data Breach.

371. Adequacy of Representation under Federal Rule of Civil Procedure (a)(4). Plaintiffs will fairly and adequately represent and protect the interests of class members, including those from states and jurisdictions where they may not reside. Plaintiffs' Counsel are competent and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

372. Predominance under Federal Rule of Civil Procedure 23(b)(3). Blackbaud has engaged in a common course of conduct toward Plaintiffs and the class members, in that all Plaintiffs' and the class members' data at issue here was stored by Blackbaud and accessed during the Data Breach. The common issues arising from Blackbaud's conduct affecting class members, as described supra, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

373. Superiority under Federal Rule of Civil Procedure 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Blackbaud. In contrast, the conduct of this action as a class

action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

374. Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2). Blackbaud has failed to take actions to safeguard Plaintiffs' and class members' Private Information such that injunctive relief is appropriate and necessary. Blackbaud has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

375. Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4). In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as Blackbaud's liability with respect to the foregoing causes of action.

## **VIII. CAUSES OF ACTION**

### **COUNT 1: NEGLIGENCE**

#### **On behalf of Plaintiffs and the Nationwide Class**

376. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

377. The Social Good Entities required Plaintiffs, Class and Subclass members to submit non-public, personal information in order to make charitable contributions to non-profit organizations, and/or obtain medical, educational, and other services.

378. In providing their Private Information, Plaintiffs, Class and Subclass members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by cybercriminals.

379. Further, Plaintiffs, Class and Subclasses members had a reasonable expectation that in the event of a data breach, Blackbaud would provide timely and adequate notice to the Social Good Entities and/or to them, and would properly identify what Private Information was exposed

during a data breach so that Plaintiffs, Class and Subclass members could take prompt and appropriate steps to safeguard their identities.

380. Blackbaud, as an entity that collects sensitive, private data from consumers such as Plaintiffs, Class and Subclass members, and likewise stores and maintains that data, has a duty arising independently from any contract to protect that information.

381. Specifically, Blackbaud, as the purported expert guardian and gatekeeper of data, had a duty to Plaintiffs, Class and Subclass members to securely maintain the Private Information collected as promised, warranted, and in a reasonable manner which would prevent cybercriminals from accessing and exfiltrating this information.

382. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Blackbaud had a duty of care to use reasonable means to secure and safeguard its systems and networks—and Plaintiffs, Class and Subclass members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

383. Blackbaud's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt and adequate notice to those affected by a data breach and/or ransomware attack.

384. Blackbaud owed a duty of care to Plaintiffs, Class and Subclass members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded the Private Information of the Plaintiffs, Class and Subclasses.

385. Blackbaud's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Blackbaud and Plaintiffs, Class and Subclass

members, the end users of the services Blackbaud provided to its clients. While this special relationship exists independent from any contract, it is recognized by Blackbaud's Privacy Policy, as well as applicable laws and regulations. Specifically, Blackbaud actively solicited Private Information as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a resulting data breach.

386. Likewise, as the guardian and gatekeeper of Plaintiffs, Class and Subclass members' Private Information, a special duty existed between Blackbaud and Plaintiffs, Class and Subclass members to promptly and adequately provide notice of the data breach and/or ransomware in a manner that would allow Plaintiffs, Class and Subclass members to take prompt and appropriate steps to safeguard their identities.

387. Blackbaud also had a common law duty to prevent foreseeable harm to others. Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiffs and class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

388. Blackbaud knew or should have known that the Plaintiffs, Class and Subclass members were relying on Blackbaud to adequately safeguard and maintain their Private Information.

389. In fact, Blackbaud publicly acknowledged Plaintiffs, Class and Subclass members' reliance on Blackbaud's duty to safeguard their Private Information in its 2019 Annual Report, Blackbaud directly addressed its myriad security obligations as well as its known susceptibility to cyberattacks. Specifically, the report states:



***If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.*** [Emphasis Added]

390. Although Blackbaud management had been repeatedly notified by employees that the systems and networks at issue in this data breach and/or ransomware were vulnerable, not secure, and that a cybercriminal attack may be successful, Blackbaud ignored the warnings and failed to improve its data safeguards and secure Plaintiffs, Class and Subclass members' Private Information.

391. Further, after discovering that cybercriminals had infiltrated its systems and networks, Blackbaud failed to timely notify the Social Good Entities or perform a proper forensic analysis of what data had been exposed, consequently, causing notice to Plaintiffs, Class, and Subclass members to be untimely and insufficient to identify what Private Information had been exposed.

392. Blackbaud had additional duties to safeguard Plaintiffs, Class and Subclass members' data through the following statutes and regulations:

- a. Pursuant to the FTC Act, 15 U.S.C. § 45, Blackbaud had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs, Class and Subclass Members' Private Information.
- b. Pursuant to HIPAA, 42 U.S.C. § 1320d, Blackbaud had a duty to securely store and maintain the Plaintiffs, Class and Subclass Members' Private Information collected in conjunction with receiving medical services.
- c. Pursuant to the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505, Blackbaud had a "mandate[d]" duty "get parental consent up front before collecting personal information from children under 13" and to "provide parents with the right to review and delete their children's information." Furthermore, under Section 312.10 of COPPA, Blackbaud could only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely

destroyed” even absent a parent’s request for the deletion of a child’s personal information.<sup>151</sup>

393. Blackbaud’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Blackbaud is bound by industry standards to protect confidential Private Information.

394. Blackbaud breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs, Class and Subclass members’ data. The specific negligent acts and omissions committed by Blackbaud include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs, Class and Subclass members’ Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to and exfiltration of Plaintiffs, Class, Subclass members’ Private Information;
- e. Failing to timely detect that Plaintiffs, Class and Subclass members’ Private Information had been compromised;
- f. Failing to perform a proper initial forensic investigation that identified what Personal Information had been compromised, resulting in inaccurate notices provided to the Social Good Entities and consequently to Plaintiffs, Class and Subclass members;
- g. Failing to provide timely notice that Plaintiffs, Class and Subclass members’ Private Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to provide adequate notice of what Private Information had been compromised so that Plaintiffs, Class and Subclass members at risk could take timely and appropriate steps to mitigate the potential for identify theft and other damages.

---

<sup>151</sup> See FTC, *Under COPPA, data deletion isn’t just a good idea. It’s the law.* (May 31, 2018), <https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law> (last visited Mar. 24, 2021).

395. It was foreseeable to Blackbaud that its failure to use reasonable measures to protect Plaintiffs, Class and Subclasses members' Private Information, including when it warned its systems and networks were vulnerable to cyberattack, would result in injury to Plaintiffs, Class and Subclass members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

396. It was additionally foreseeable to Blackbaud that failure to timely and adequately provide notice of the Data Breach would result in Plaintiffs, Class and Subclass members not being afforded the ability to timely safeguard their identities.

397. It was therefore foreseeable to Blackbaud that its failure to adequately safeguard Plaintiffs, Class and Subclass members' Private Information or provide timely and adequate notice of the Data Breach, would result in one or more types of injuries to Plaintiffs, Class and Subclasses members.

398. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

399. Plaintiffs are also entitled to injunctive relief requiring Blackbaud to, e.g., (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class members, and any other relief this Court deems just and proper.

**COUNT 2: NEGLIGENCE *PER SE***  
**On behalf of Plaintiffs and the Nationwide Class**

400. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

401. Blackbaud had duties to safeguard Plaintiffs, Class and Subclass members' data that arose through certain statutes and regulations.

402. Pursuant to the FTC Act, 15 U.S.C. § 45, Blackbaud had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs, Class and Subclass members' Private Information. Similar state-specific statutory causes of action—such as consumer fraud and unfair trade practices acts—provide for such a duty, as well.

403. Pursuant to HIPAA, 42 U.S.C. § 1320d, Blackbaud had a duty to securely store and maintain the Plaintiffs, Class and Subclass Members' Private Information collected in conjunction with receiving medical services.

404. Pursuant to the COPPA, 15 U.S.C. §§ 6501-6505, Blackbaud had a duty to: (i) get parental consent before collecting personal information from children under 13; (ii) provide parents with the right to review and delete their children's information; and (iii) could only retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected, and thereafter had a duty to delete any and all children's personal information using reasonable measures to ensure it's been securely destroyed, even absent a parent's request for the deletion of a child's personal information.

405. Plaintiffs, Class and Subclass members are members of the classes of persons the foregoing statutes and regulations are intended to protect.

406. The essential purposes of these statutes are to protect from the same or similar kind of harm caused to Plaintiffs, Class and Subclass members, as a direct and proximate result of Blackbaud's breach of those statutory and regulatory duties.

407. Blackbaud breached its duties to Plaintiffs, Class and Subclass members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs, Class and Subclass members' Private Information.

408. Blackbaud breached its duties to minor Plaintiffs, Class and Subclass members under the COPPA by failing (1) to provide fair, reasonable, or adequate computer systems and data security practices to safeguard minor Plaintiffs, Class and Subclass members' Private Information; (2) to obtain parental consent before collecting personal information from children under the age of 13; (3) to provide parents the right to review and delete their children's' information; and (4) timely and properly delete any and all children's' personal information using reasonable measures to ensure it's been securely destroyed.

409. Blackbaud's breach of its duties arising out of the foregoing statutes and regulations constitutes negligence per se.

410. But for Blackbaud's wrongful and negligent breach of its duties owed to Plaintiffs, Class and Subclass members, Plaintiffs, Class and Subclass members' data would not have been compromised and they would not have been harmed.

411. The injury and harm suffered by Plaintiffs, Class and Subclass members was the reasonably foreseeable result of Blackbaud's breach of its duties. Blackbaud knew or should have known that it was failing to meet its duties, and that Blackbaud's breach would cause Plaintiffs and the class and Subclasses members to experience the foreseeable harms associated with the exposure of their Private Information, including increased risk of identity theft.

412. As a direct and proximate result of Blackbaud's violation of the foregoing statutes and regulations, Plaintiffs, Class and Subclasses members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

**COUNT 3: GROSS NEGLIGENCE**  
**On behalf of Plaintiffs and the Nationwide Class**

413. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

414. Plaintiffs were required to submit non-public Private Information in order to make charitable contributions to the Social Good Entities, and/or obtain medical, educational, and other services. Blackbaud had a duty to Plaintiffs to securely maintain the Private Information collected as promised and warranted.

415. However, Blackbaud maintained unencrypted Personal Information on certain programs. Blackbaud also maintained outdated, legacy versions of its Educational Edge and other programs which were no longer in active use.

416. Blackbaud knew this information was (a) unencrypted and thus subject to breach and misuse; (b) could not be seen by the Social Good Entities; (c) included highly sensitive Private Information; and (d) was “at rest,” meaning the data was not in transit and being actively used.

417. The failure to encrypt this “at rest” obsolete data containing highly sensitive Personal Information on legacy and/or back-up versions of Blackbaud systems was particularly flagrant and egregious. Indeed, this unencrypted Private Information on legacy and/or back-up versions made public exposure of this Private Information in a cyberattack very likely.

418. Moreover, there was no reasonable reason for retaining these records which contain highly sensitive Private Information, including SSNs. Blackbaud has, in fact, acknowledged its failure to encrypt this highly sensitive Private Information.

419. Thus, despite Blackbaud’s initial representations that no sensitive Personal Information was accessed, the highly sensitive, unencrypted Personal Information of Plaintiffs was accessed, exfiltrated and otherwise exposed by the Data Breach.

420. By voluntarily accepting the duty to maintain and secure this data, and sharing it and using it for commercial gain, Blackbaud had a duty of care to use reasonable means to secure

and safeguard its computer systems to prevent disclosure of the information, and to safeguard the information from cyber theft.

421. Blackbaud's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach and/or ransomware attack.

422. Blackbaud owed a duty of care to Plaintiffs to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded Plaintiffs' Private Information.

423. Blackbaud owed an additional duty to Plaintiffs to take measures to ensure that, *inter alia*:

- a. all Private Information was encrypted and continued to be encrypted;
- b. "at rest" data is deleted after a reasonable amount of time; and/or
- c. Social Good Entities and Plaintiffs were notified that their "at rest," sensitive and unencrypted Private Information had continued to be stored.

424. Blackbaud's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Blackbaud and Plaintiffs, the end users of the services Blackbaud provided to its clients, which is recognized by Blackbaud's Privacy Policy, as well as applicable laws and regulations. Blackbaud actively solicited Private Information as part of its business and was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs from a ransomware attack and resulting data breach.

425. Pursuant to the FTC Act, 15 U.S.C. § 45, Blackbaud had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and the class members' Private Information. Plaintiffs and the class members are the individuals whom the FTC Act is intended to protect.

426. Pursuant to HIPAA, 42 U.S.C. § 1320d, Blackbaud had a duty to securely store and maintain Plaintiffs' and the class members' Private Information. Plaintiffs and the class members are the individuals whom HIPAA is intended to protect.

427. Pursuant to the COPPA, 15 U.S.C. §§ 6501-6505, Blackbaud had a duty to: (i) get parental consent before collecting personal information from children under 13; (ii) provide parents with the right to review and delete their children's information; and (iii) could only retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected, and thereafter had a duty to delete any and all child's personal information using reasonable measures to ensure it's been securely destroyed, even absent a parent's request for the deletion of a child's personal information. Minor Plaintiffs and minor class members are the individuals whom COPPA is intended to protect.

428. Blackbaud's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Blackbaud is bound by industry standards to protect confidential Private Information.

429. Blackbaud consciously failed to use reasonable measures to protect Plaintiffs and class members' data. The specific gross negligent acts and omissions committed by Blackbaud include, but are not limited to, the following:

- a. Consciously failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and class members' Private Information;
- b. Consciously failing to ensure all sensitive Personal Information was encrypted;
- c. Consciously failing to ensure all "at rest" data was destroyed in a reasonable amount of time;
- d. Consciously failing to notify the Social Good Entities, Plaintiffs, and class members that unencrypted, "at rest" data was still maintained by Blackbaud;
- e. Consciously failing to adequately monitor the security of its networks and systems;



- f. Consciously failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- g. Consciously allowing unauthorized access to class members' Private Information;
- h. Consciously failing to detect in a timely manner that class members' Private Information had been compromised; and
- i. Consciously failing to timely notify Plaintiffs and class members about the Data Breach so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

430. It was foreseeable that Blackbaud's conscious failure to use reasonable measures to protect the Plaintiffs class members' Private Information would result in injury to the Plaintiffs and class members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

431. It was therefore foreseeable that the conscious failure to adequately safeguard the Plaintiffs and class members' Private Information would result in one or more types of injuries to Plaintiffs and class members.

432. Blackbaud paid a ransom to ensure that cybercriminals did not publish Plaintiffs' and class members' data. As a result, cybercriminals now know that the Private Information of Plaintiffs and class members is valuable enough to fetch a ransom. It is thus foreseeable that, in making a ransom payment, Blackbaud is subjecting Plaintiffs and class members to further targeting by cybercriminals' further demands for ransom from the Plaintiffs and class members, as well as identity theft and fraud.

433. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

434. Plaintiffs and class members are also entitled to injunctive relief requiring Blackbaud to, e.g., (i) identify all legacy data it still maintains; (ii) destroy or encrypt legacy data that has been "at rest" for an unreasonable amount of time; (iii) notify all Social Good Entities and

consumers with legacy data that is still be maintained by Blackbaud; (iv) strengthen its data security programs and monitoring procedures; (v) submit to future annual audits of those systems and monitoring procedures; and (vi) immediately provide robust and adequate credit monitoring to Plaintiffs Class members, and any other relief this Court deems just and proper.

**COUNT 4: UNJUST ENRICHMENT**  
**On behalf of Plaintiffs and the Nationwide Class**

435. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

436. Plaintiffs, the Class and Subclass members have an interest, both equitable and legal, in the Private Information about them that was collected, secured, and maintained by Blackbaud and that was ultimately compromised in the Data Breach.

437. A financial benefit was conferred upon Blackbaud when Plaintiffs, the Class and Subclass members provided their Private Information to the Social Good Entities in conjunction with donating money or for medical services. Blackbaud's business model would not exist save for the need to ensure the security of Plaintiffs' and class members' Private Information.

438. The relationship between Blackbaud and Plaintiffs, the Class and Subclass members is not attenuated, as Plaintiffs, the Class and Subclass members had a reasonable expectation that the security of their information would be maintained when they provided their information to Social Good Entities. Plaintiffs, the Class and Subclass members were induced to provide their information in reliance on the fact that Blackbaud's stated data security measures were adequate.

439. Upon information and belief, this financial benefit was, in part, conferred when portions of Plaintiffs, Class and Subclass members' donations were used by the Social Good Entities to pay Blackbaud for maintenance of the platforms, payment modules used to collect the donations, and monthly service fees.

440. Upon information and belief, Blackbaud retained a portion of Plaintiffs, Class and Subclass members' donations paid in conjunction with Blackbaud collecting and maintaining the Plaintiffs, the Class and Subclass members' Private Information.

441. Blackbaud realized the benefit of the portion of donations and money collected by the Social Good Entities and used to pay for Blackbaud's maintenance of the platforms, payment modules and monthly service fees.

442. Blackbaud also understood and appreciated that the Private Information pertaining to Plaintiffs, the Class and Subclasses members was private and confidential and its value depended upon Blackbaud maintaining the privacy and confidentiality of that Private Information.

443. In fact, Blackbaud publicly represented that value in its 2019 Annual Report, Blackbaud when it addressed that if it "fail[s] to securely collect, store and transmit customer information, or [it] fail[s] to safeguard confidential donor data, [it] could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer."

444. But for Blackbaud's willingness and commitment to properly and safely collect, maintain and secure the Private Information would not have been transferred to and entrusted with Blackbaud. Further, if Blackbaud had disclosed that its data security measures were inadequate, Blackbaud would not have gained the trust of the Social Good Entities.

445. As a result of Blackbaud's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs, the Class and Subclass members without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), Blackbaud has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs, the Class and Subclasses members. Among other things, Blackbaud

continues to benefit and profit from the sale of the Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

446. Blackbaud's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiffs, the Class and Subclasses members' sensitive Private Information, while at the same time failing to maintain that information secure from unauthorized access and exfiltration by cyber criminals.

447. It would be unjust, inequitable, and unconscionable for Blackbaud to be permitted to retain the benefits it received, and is still receiving, from Plaintiffs, the Class and Subclasses members in connection with the collection, maintenance and security of their Private Information. Blackbaud's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

448. The benefit conferred upon, received, and enjoyed by Blackbaud was not conferred officiously or gratuitously, and it would be inequitable and unjust for Blackbaud to retain the benefit.

449. Blackbaud is therefore liable to Plaintiffs, the Class and Subclasses members for restitution in the amount of the benefit conferred on Blackbaud as a result of its wrongful conduct, including specifically the value to Blackbaud of the Private Information that was stolen in the Data Breach and the profits Blackbaud is receiving from the use and sale of that information.

**COUNT 5: DECLARATORY JUDGMENT**  
**On behalf of Plaintiffs and the Nationwide Class**

450. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

451. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

452. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard Plaintiffs, Class and Subclass members' Private Information and whether Blackbaud is currently maintaining data security measures adequate to protect Plaintiffs, the Class and Subclasses members from further, future data breaches that compromise their Private Information.

453. Plaintiffs, Class and Subclass members allege that Blackbaud's data security measures remain inadequate and Blackbaud has not provided any evidence that it has remedied the failure that occurred in the Data Breach at issue or has remedied any other vulnerability from its failure to properly assess threats by cybercriminals.

454. Plaintiffs, the Class and Subclass members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

455. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Blackbaud continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the FTC Act, HIPAA, COPPA, and various state statutes;
- b. Blackbaud owes a duty by virtue of its special relationship, understanding that it is safeguarding sensitive, Private Information, or that it has already acknowledged a responsibility to keep such information safe by virtue of security policies; and
- c. Blackbaud continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

456. The Court also should issue corresponding prospective injunctive relief requiring Blackbaud to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

457. If an injunction is not issued, Plaintiffs, the Class and Subclass members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Blackbaud. The risk of another such breach is real, immediate, and substantial. If another breach at Blackbaud occurs, Plaintiffs, the Class and Subclass members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

458. The hardship to Plaintiffs, the Class and Subclass members if an injunction does not issue exceeds the hardship to Blackbaud if an injunction is issued. Among other things, if another massive data breach occurs at Blackbaud, Plaintiffs, the Class and Subclass members will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to Blackbaud of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Blackbaud has a pre-existing legal obligation to employ such measures.

459. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach at Blackbaud, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

**COUNT 6: INVASION OF PRIVACY**  
**On behalf of Plaintiffs and the Nationwide Class**

460. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

461. Plaintiffs, Class and Subclass members have a legally protected privacy interest in their Private Information, which is and was collected, stored and maintained by Blackbaud, and they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access, as occurred with the Data Breach.

462. Plaintiffs, Class and Subclass members reasonably expected that Blackbaud would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

463. Blackbaud unlawfully invaded the privacy rights of Plaintiffs, Class and Subclasses members by engaging in the conduct described above, including by failing to protect their Private Information by permitting unauthorized third-parties to access, exfiltrate and view this Private Information. Likewise, Blackbaud further invaded the privacy rights of Plaintiffs, Class and Subclass members, and permitted cybercriminals to invade the privacy rights of Plaintiffs, Class and Subclass members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what Private Information had been accessed, exfiltrated, and viewed by unauthorized third-parties.

464. This invasion of privacy resulted from Blackbaud's failure to properly secure and maintain Plaintiffs, the Class and Subclasses members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

465. Plaintiffs, the Class and Subclasses members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs,

the Class and Subclasses members' Private Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

466. The disclosure of Plaintiffs, the Class and Subclasses members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

467. Blackbaud's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class and Subclasses members' sensitive, Private Information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

468. The unauthorized access, exfiltration, and disclosure of Plaintiffs, the Class and Subclasses members' Private Information was without their consent, and in violation of various statutes, regulations and other laws.

469. As a result of the invasion of privacy caused by Blackbaud, Plaintiffs, the Class and Subclass members suffered and will continue to suffer damages and injury as set forth herein.

470. Plaintiffs, the Class and Subclasses members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

**COUNT 7: VIOLATION OF STATE CONSUMER PROTECTION LAWS, DECEPTIVE  
BUSINES PRACTICES ACTS, AND DATA BREACH NOTIFICATION STATUTES  
On behalf of Plaintiffs and the Nationwide Class**

471. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

472. Each of the jurisdictions described herein has passed a statutory consumer protection law or unfair and deceptive trade practices law.

473. Blackbaud is a "person" under those statutes, and Plaintiffs and Class members are "consumers."



474. Blackbaud is on notice of the allegations contained herein.

475. Blackbaud engaged in deceptive acts and practices in the conduct of trade or commerce, and violations of data breach notification statutes including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;
- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, 15 U.S.C. § 45(a)(1), 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05; and
- d. Failing to notify consumers of a data breach within a reasonable period of time, as applicable statutes allow.

476. Blackbaud's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Class members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Private Information;
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;
- j. Failing to discover the Data Breach within a reasonable period of time; and
- k. Failing to provide notice of the Data Breach within a reasonable period of time in accordance with statutes.

477. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

478. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class members, that their Private Information was not exposed and misled Plaintiffs and the Class members into believing they did not need to take actions to secure their identities.

479. Blackbaud intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

480. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

481. Instead, Blackbaud continued to be trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and the Class. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

482. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Class members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

483. Blackbaud acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Class members' rights.

484. As a direct and proximate result of Blackbaud's deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

485. Blackbaud's deceptive acts and practices caused substantial injury to Plaintiffs, and Class members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

486. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

#### **CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS**

##### **COUNT 8: CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq.***

487. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges the foregoing paragraphs 1-375 as if fully alleged herein. This claim is brought individually under the laws of California and

on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

488. “[T]o ensure that Personal Information about California residents is protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure.”

489. Blackbaud is a business that owns, maintains, and licenses “personal information”, within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiff and California Subclass members.

490. Blackbaud is registered as a “data broker” in California, which is defined as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” Cal. Civ. Code § 1798.99.80.152

491. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of Personal Information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82. Id.

---

<sup>152</sup> <https://oag.ca.gov/data-broker/registration/185724>

492. Blackbaud is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

493. Plaintiff and California Subclass members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

494. Because Blackbaud reasonably believed that Plaintiff and California Subclass members' Private Information was acquired by unauthorized persons during the Data Breach, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

495. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Cal. Civ. Code § 1798.82.

496. As a direct and proximate result of Blackbaud's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

497. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

**COUNT 9: CALIFORNIA UNFAIR COMPETITION LAW,  
Cal. Bus. & Prof. Code §§ 17200, *et seq.***

498. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

499. Blackbaud is a "person" as defined by Cal. Bus. & Prof. Code §17201.

500. Blackbaud violated Cal. Bus. & Prof. Code §§ 17200, et seq. (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

501. Blackbaud’s “unfair” and “deceptive” acts and practices include:

- a. Blackbaud failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members’ Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Blackbaud failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, Blackbaud failed to patch the well-known Apache Struts vulnerability, which made it trivial for a hacker to penetrate Blackbaud’s systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Private Information has been compromised.
- b. Blackbaud’s failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers’ data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including California’s Consumer Legal Remedies Act (“CLRA”), Cal Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Confidentiality of Medical Information Act (“CMIA”), Cal Civ. Code § 56.26(b), and California’s Consumer Records Act, Cal. Civ. Code § 1798.81.5.
- c. Blackbaud’s failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Blackbaud’s inadequate security, consumers could not have reasonably avoided the harms that Blackbaud caused.
- d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

502. Blackbaud has engaged in “unlawful” business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, et seq., the CLRA, Cal. Civ. Code §§ 1780, et seq., 15 U.S.C. § 680, et seq., the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

503. Blackbaud’s unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and California Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

504. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

505. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

506. As a direct and proximate result of Blackbaud's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

507. Blackbaud acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights.

508. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Blackbaud's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.



**COUNT 10: CALIFORNIA CONSUMER LEGAL REMEDIES ACT,  
Cal. Civ. Code §§ 1750, *et seq.***

509. The California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

510. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (“CLRA”) is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

511. Blackbaud is a “person” as defined by Civil Code §§ 1761(c) and 1770, and has provided “services” as defined by Civil Code §§ 1761(b) and 1770. Specifically, Blackbaud provides cloud-based computing services to customers that involve storing and managing Private Information for use by consumers and direct customers such as Social Good Entities.

512. As part of the services Blackbaud offers, Blackbaud touts its ongoing efforts to keep consumers’ Private Information secure, including by ensuring ongoing compliance with legal privacy standards established both domestically and abroad, as recognized by Blackbaud’s Privacy Shield Notice. Indeed, Blackbaud purports to “tirelessly track and interpret pending legislation to ensure that that Blackbaud provides the features [customers] need to protect the privacy of [their] constituents while managing data in a compliant way. As privacy legislation evolves, [Blackbaud’s] products do too.”

513. Plaintiffs and the California Class are “consumers” as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

514. Blackbaud’s acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.
- e. Blackbaud violated Civil Code § 1770, in the following ways:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);

- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and California Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, et seq., HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

515. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

516. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

517. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the California Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the

California Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

518. As a direct and proximate result of Blackbaud's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

519. Plaintiffs and the California Subclass have provided notice of their claims for damages to Blackbaud, in compliance with California Civil Code § 1782(a), on February 24, 2021. Blackbaud responded on March 8, 2021; however, such response did not offer or provide an adequate remedy at law.

520. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

**COUNT 11: CALIFORNIA CONSUMER PRIVACY ACT,  
Cal. Civ. Code §§ 1798.100, *et seq.***

521. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

522. Plaintiffs and California Subclass members are residents of California.

523. Blackbaud is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over \$25 million.

524. Blackbaud is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Blackbaud obtains, receives, or accesses consumers' personal information when customers use Blackbaud's products to maintain and process consumer data.

525. Blackbaud and its direct customers determine the purposes and means of processing consumers' personal information. Blackbaud uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test Blackbaud's services.

526. Blackbaud is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.

527. Blackbaud violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs and the California Subclass members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Blackbaud's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

528. Blackbaud knew or should have known that its data security practices were inadequate to secure California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

529. Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

530. The cybercriminals accessed “nonencrypted and unredacted personal information” as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

531. Upon information and belief, Plaintiff and California Subclass members’ Private Information accessed by the cybercriminals in the Data Breach includes “nonencrypted and unredacted personal information” as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

532. Plaintiffs seek injunctive relief in the form of an order requiring Blackbaud to employ adequate security practices consistent with law and industry standards to protect the California Subclass members’ Private Information, requiring Blackbaud to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members’ authorization, along with an explanation of how the data breach occurred.

533. Plaintiffs and the California Subclass members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

534. As a direct and proximate result of Blackbaud’s violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

535. On September 9, 2020, counsel for Mamie Estes served written notice identifying Blackbaud’s violations of Cal. Civil Code § 1798.150(a) and demanding the data breach be cured, pursuant to Cal. Civil Code § 1798.150(b). On September 11, 2020, counsel for Philip Eisen, Mamie Estes, Shawn Regan and Kassandre Clayton, respectively, did the same. Because Blackbaud has neither cured the noticed violation nor and provided the Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur, Plaintiff and the California Subclass seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

**COUNT 12: CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT,  
Cal. Civil Code § 56, et seq.**

536. The California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

537. The California’s Confidentiality of Medical Information Act (“CMIA”) prohibits, among other things, unauthorized disclosure of private medical information. Cal. Civ. Code §§ 56, et seq.

538. Plaintiffs provided their PHI to a Social Good Entity which is a “health care practitioner” is a “provider of health care” as defined by Cal. Civ. Code § 56.05(j).

539. Plaintiffs are “patients” as defined by Cal. Civ. Code § 56.05(k).

540. Blackbaud is a “provider of health care” subject to the CMIA because it is a “business that offers software or hardware to consumers, . . . that is designed to maintain medical information” in order to make the information available to an individual or Social Good Entity to which Plaintiff provided her PHI. Cal. Civ. Code § 56.06(b).

541. Blackbaud stored in electronic form on its computer system Plaintiffs’ “medical information” as defined by Cal. Civ. Code § 56.05(j).

542. Blackbaud’s systems were designed, in part, to make medical information available to Social Good Entities by providing cloud-based computing solutions through which those organizations could store, access, and manage consumers’ medical information, including but not limited to diagnosing, treating, or managing consumers’ medical conditions.

543. Plaintiff did not provide Blackbaud authorization nor was Blackbaud otherwise authorized to disclose Plaintiff's medical information to an unauthorized third-party.

544. As described throughout this Complaint, Blackbaud negligently maintained, disclosed and released Plaintiff's and the California PHI Subclass members' medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

545. As a direct and proximate result of Blackbaud's negligence, it disclosed and released Plaintiff's and the California PHI Subclass members' medical information to an unauthorized third-party.

546. Blackbaud's unauthorized disclosure of medical records has caused injury to the Plaintiff and the California PHI Subclass.

547. Upon information and belief, Plaintiff's confidential medical information was viewed by an unauthorized third party.

548. Accordingly, Plaintiff, individually and on behalf of members of the California PHI Subclass, seek to recover actual, nominal (including \$1000 nominal damages per disclosure under § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS**

#### **COUNT 13: ILLINOIS CONSUMER FRAUD ACT, 815 ILCS §§ 505, *et seq.***

549. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-375, as if fully



alleged herein. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

550. Blackbaud is a “person” as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

551. Plaintiff and Illinois Subclass members are “consumers” as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

552. Blackbaud’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. § 505/1(f).

553. Blackbaud’s deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of

Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Illinois Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).
- j. By failing to provide disclose the Data Breach in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

554. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

555. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Illinois Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

556. Blackbaud intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

557. The above unfair and deceptive practices and acts by Blackbaud offend public policy, and were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

558. Blackbaud acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights.

559. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

560. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

**COUNT 14: ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,  
815 ILCS §§ 510/2, *et seq.***

561. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

562. Blackbaud is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

563. Blackbaud engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;

- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

564. Blackbaud's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Illinois Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Private Information; and

- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a)).

565. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

566. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Illinois Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

567. The above unfair and deceptive practices and acts by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

568. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

569. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

**CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS**

**COUNT 15: MARYLAND CONSUMER PROTECTION ACT,  
Md. Comm. Code §§ 13-301, *et seq.***

570. The Maryland Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Maryland and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

571. Blackbaud is a person as defined by Md. Comm. Code § 13-101(h).

572. Blackbaud’s conduct as alleged herein related to “sales,” “offers for sale,” or “bailment” as defined by Md. Comm. Code § 13-101(i) and § 13-303.

573. Maryland Subclass members are “consumers” as defined by Md. Comm. Code § 13-101(c).

574. Blackbaud’ advertises, offers, or sell “consumer goods” or “consumer services” as defined by Md. Comm. Code § 13-101(d).

575. Blackbaud advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

576. Blackbaud engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

- a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;
- b. Representing that consumer goods or services have a characteristic that they do not have;
- c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;
- d. Failing to state a material fact where the failure deceives or tends to deceive;

- e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
- f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

577. Blackbaud engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of Md. Comm. Code § 13-303, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maryland Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maryland Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Maryland Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland Subclass members' Private Information; and

- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.
- j. Failing to take reasonable steps to protect against the unauthorized access or use of the personal information belonging to Plaintiff and Maryland Subclass members in violation of the Maryland Personal Information Protection Act, Md. Comm. Code §§14-3501 et seq.
- k. Publicly posting or displaying Social Security numbers belonging to the Plaintiff and Maryland Subclass members in violation of the Social Security Number Privacy Act, Md. Comm. Code §14-3401 *et. seq.*

578. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information. Blackbaud's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

579. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Maryland Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Maryland Subclass members into believing they did not need to take actions to secure their identities.

580. Blackbaud intended to mislead Plaintiff and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

581. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Maryland Subclass.



Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Maryland Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

582. Blackbaud acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass members' rights.

583. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

584. Plaintiff and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

**COUNT 16: MARYLAND CONFIDENTIALITY OF MEDICAL RECORDS ACT,  
Md. Health-Gen. Code § 4-301, *et seq.***

585. The Maryland Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland PHI Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Maryland and on behalf of all other natural persons whose Private Information was compromised as a result of the

Data Breach and reside in states having similar laws regarding the confidentiality of medical records.

586. The Maryland Confidentiality of Medical Record Act (“MCMRA”) prohibits, among other things, unauthorized disclosure of private medical records. Md. Code Health-Gen. § 4-302(a).

587. Plaintiff provided her PHI to a Social Good Entity which is a “health care provider” as defined by Md. Code Health-Gen. § 4-301(g)(1).

588. Blackbaud is an “agent” of the Social Good Entity to which Plaintiff provided her PHI and therefore is a health care provider as defined by Md. Code Health-Gen. § 4-301(g)(1).

589. Blackbaud is also “person” to whom medical records are disclosed as defined by MD Code Health-Gen. § 4-302, and therefore subject to the requirements of the MCMRA.

590. Plaintiff [] is a “patient”, as defined by Md. Code Ann., Health-Gen. § 4-301(k), of the Social Good Entity to which she provided her PHI.

591. Blackbaud stored on its computer system “medical records” as defined by Md. Code Health-Gen. § 4-301(h)(i)(1) pertaining to the Plaintiff and the Maryland PHI Subclass.

592. Blackbaud disclosed medical records pertaining to the Plaintiff and the Maryland PHI Subclass without their authorization and for no other reason permitted by Md. Code Health-Gen. § 4-302, and therefore violated Md. Code Health-Gen. § 4-302.

593. Disclosure of medical records to unauthorized individuals resulted from the affirmative actions of Blackbaud in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private medical records of the Plaintiff and the Maryland PHI Subclass.

594. Blackbaud's unauthorized disclosure of medical records has caused injury to the Plaintiff and the Maryland PHI Subclass.

595. The Plaintiff and the Maryland PHI Subclass seek relief pursuant to Md. Code Health-Gen. § 4-309, including actual damages for Blackbaud's knowing violations of Md. Code Health-Gen. § 4-302.

### **CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS**

#### **COUNT 17: MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, *et seq.***

596. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Michigan and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding identity theft protection.

597. Blackbaud is a business that owns or licenses computerized data that includes "personal information" as defined by Mich. Comp. Laws Ann. § 445.72(1).

598. Plaintiff's and Michigan Subclass members' Private Information includes "personal information" as covered under Mich. Comp. Laws Ann. § 445.72(1).

599. Blackbaud is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

600. Because Blackbaud discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized

persons), Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

601. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Mich. Comp. Laws Ann. § 445.72(4).

602. As a direct and proximate result of Blackbaud's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as described above.

603. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

**COUNT 18: MICHIGAN CONSUMER PROTECTION ACT,  
Mich. Comp. Laws Ann. §§ 445.903, *et seq.***

604. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Michigan and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

605. Blackbaud and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

606. Blackbaud advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

607. Blackbaud engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
- c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and
- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).
- e. Blackbaud's unfair, unconscionable, and deceptive practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Michigan Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Michigan Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 1681e, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

608. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

609. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Michigan Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Michigan Subclass members into believing they did not need to take actions to secure their identities.

610. Blackbaud intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

611. Blackbaud acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights.

612. As a direct and proximate result of Blackbaud's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

613. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS**

**COUNT 19: NEW YORK GENERAL BUSINESS LAW,  
N.Y. Gen. Bus. Law §§ 349, *et seq.***

614. The New York Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of New York and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive acts or practices.

615. Blackbaud engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and New York Subclass members of the Data Breach;

- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

616. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

617. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New York Subclass members, that their Private Information was not exposed and misled Plaintiffs and the New York Subclass members into believing they did not need to take actions to secure their identities.

618. Blackbaud acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights.

619. As a direct and proximate result of Blackbaud's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.



620. Blackbaud's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

621. The above deceptive and unlawful practices and acts by Blackbaud caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

622. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

#### **CLAIMS ON BEHALF OF THE OHIO SUBCLASS**

##### **COUNT 20: OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq.***

623. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Ohio and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

624. Blackbaud, Plaintiff, and Ohio Subclass members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

625. Blackbaud advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

626. Blackbaud engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

- a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);
- b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and
- c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).
- d. Blackbaud's deceptive trade practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Ohio Subclass members of the Data Breach;
- k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Private Information; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

627. Blackbaud did not engage in reasonable data security measures and/or did not follow its own data security measures in place at the time of the Data Breach.

628. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

629. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Ohio Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Ohio Subclass members into believing they did not need to take actions to secure their identities.

630. Blackbaud intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

631. Blackbaud acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights.

632. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

633. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE OREGON SUBCLASS**

**COUNT 21: OREGON UNLAWFUL TRADE PRACTICES ACT,  
Or. Rev. Stat. §§ 646.608, *et seq.***

634. The Oregon Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Oregon and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unlawful trade practices.

635. Blackbaud is a “person,” as defined by Or. Rev. Stat. § 646.605(4).

636. Blackbaud engaged in the sale of “goods and services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

637. Blackbaud sold “goods or services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

638. Blackbaud advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

639. Blackbaud engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

- a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);
- b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);
- c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and
- d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).
- e. Blackbaud’s unlawful practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;

- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;
- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Oregon Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

640. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

641. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Oregon Subclass members, that their

Private Information was not exposed and misled Plaintiffs and the Oregon Subclass members into believing they did not need to take actions to secure their identities.

642. Blackbaud intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

643. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Oregon Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Oregon Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

644. Blackbaud acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights.

645. As a direct and proximate result of Blackbaud's unlawful practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

646. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of \$200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS**

**COUNT 22: SOUTH CAROLINA DATA BREACH SECURITY ACT,  
S.C. Code Ann. §§ 39-1-90, *ET SEQ.***

647. The South Carolina Plaintiff(s) identified above ("Plaintiff(s)," for purposes of this Count), individually and on behalf of the Nationwide Class and South Carolina Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of South Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding data breach security.

648. Blackbaud is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

649. Plaintiffs, the Class and South Carolina Subclass members' Private Information includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

650. Blackbaud is required to adequately notify Plaintiffs, the Class and South Carolina Subclass members following discovery or notification of a breach of its data security program if Private Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

651. Because Blackbaud discovered a breach of its data security program in which Private Information that was not rendered unusable through encryption, redaction, or other

methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

652. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated S.C. Code Ann. § 39-1-90(A).

653. As a direct and proximate result of Blackbaud's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff, the Class and South Carolina Subclass members suffered damages, as described above.

654. Plaintiff, the Class and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

#### **CLAIMS ON BEHALF OF THE TEXAS SUBCLASS**

##### **COUNT 23: DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.***

655. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

656. Blackbaud is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

657. Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

658. Blackbaud advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).



659. Blackbaud engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.
- d. Blackbaud's false, misleading, and deceptive acts and practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;
- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;
- j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Texas Subclass members of the Data Breach;
- k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Private Information; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

660. Blackbaud intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

661. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

662. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Texas Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Texas Subclass members into believing they did not need to take actions to secure their identities.

663. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Texas Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Texas Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

664. Blackbaud had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally

accepted professional standards in its industry. This duty arose because members of the public, including Plaintiffs and the Texas Subclass, repose a trust and confidence in Blackbaud. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Blackbaud because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

665. Blackbaud engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Blackbaud engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

666. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Blackbaud's data security because this information was known exclusively by Blackbaud. Consumers also lacked the ability, experience, or capacity to secure the Private Information in Blackbaud's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Blackbaud's systems in order to evaluate its security controls. Blackbaud took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Private Information.

667. Blackbaud intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Blackbaud's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Blackbaud's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

668. Blackbaud acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights.

669. As a direct and proximate result of Blackbaud's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information. Blackbaud's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

670. Blackbaud's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

671. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

**COUNT 24: TEXAS HEALTH & SAFETY CODE § 241.152**

672. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas PHI Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding health and safety.

673. Plaintiff brings this cause of action in the District Court of South Carolina as the Judicial Panel on Multidistrict Litigation created this MDL, and this Court is handling all pretrial matters related to the Data Breach and causes of action alleged concerning same.

674. Texas law provides that, except under circumstances that do not apply here, a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative. See Tex. Health & Safety Code § 241.152.

675. At all relevant times, the Social Good Entity to which Plaintiff provided his PHI was a "hospital" within the meaning of Tex. Health & Safety Code § 241.152.

676. At all relevant times, Blackbaud stored "health care information" of the Plaintiff and other members of the Texas PHI Subclass as construed under Tex. Health & Safety Code § 241.153.

677. Plaintiff and the other Texas PHI Subclass members did not provide Blackbaud consent to release their health care records to third parties.

678. Blackbaud had a duty to adopt and implement reasonable safeguards for the security of all health care information it maintains pursuant to Tex. Health & Safety Code § 241.155.

679. Blackbaud negligently or intentionally disclosed and released Plaintiff's and the Texas PHI Subclass members' health care information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to health care information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

680. As a direct and proximate result of Blackbaud's negligent or intentional acts, it disclosed and released Plaintiff's health care information to third parties without the Plaintiff's consent and caused injury to the Plaintiff and the Texas PHI Subclass.

681. Accordingly, Plaintiff, individually and on behalf of members of the Texas PHI Subclass, seeks compensatory damages, injunctive relief plus costs and attorney fees. See Tex. Health & Safety Code § 241.156.

### **CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS**

#### **COUNT 25: VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT, Va. Code. Ann. §§ 18.2-186.6, *et seq.***

682. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Virginia and on behalf

of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding personal information.

683. Blackbaud is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security program if unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

684. Blackbaud is an entity that owns or licenses computerized data that includes “personal information” as defined by Va. Code Ann. § 18.2-186.6(B).

685. Plaintiff’s and Virginia Subclass members’ Private Information includes “personal information” as covered under Va. Code Ann. § 18.2-186.6(A).

686. Because Blackbaud discovered a breach of its security system in which unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

687. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Va. Code Ann. § 18.2-186.6(B).

688. As a direct and proximate result of Blackbaud’s violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

689. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

**COUNT 26: VIRGINIA CONSUMER PROTECTION ACT,  
Va. Code Ann. §§ 59.1-196, *et seq.***

690. The Virginia Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-375, as if fully alleged herein. This claim is brought individually under the laws of Virginia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

691. The Virginia Consumer Protection Act prohibits “[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.” Va. Code Ann. § 59.1-200(14).

692. Blackbaud is a “person” as defined by Va. Code Ann. § 59.1-198.

693. Blackbaud is a “supplier,” as defined by Va. Code Ann. § 59.1-198.

694. Blackbaud engaged in the complained-of conduct in connection with “consumer transactions” with regard to “goods” and “services,” as defined by Va. Code Ann. § 59.1-198.

695. Blackbaud engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virginia Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;



- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virginia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Virginia Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virginia Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

696. Blackbaud intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

697. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Subclass members, about the adequacy of Blackbaud's computer and data security and the quality of the Blackbaud brand.

698. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Virginia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Georgia Subclass members into believing they did not need to take actions to secure their identities.

699. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Virginia Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Virginia Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

700. In Blackbaud had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

701. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

- a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;
- b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

- c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

702. Blackbaud acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. An award of punitive damages would serve to punish Blackbaud for its wrongdoing, and warn or deter others from engaging in similar conduct.

703. As a direct and proximate result of Blackbaud's deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

704. Blackbaud's violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

705. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of \$1,000 per violation if the conduct is found to be willful or, in the alternative, \$500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

#### **IX. PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and Subclasses;
- B. For equitable relief enjoining Blackbaud from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the class

and Subclass members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and the class members or to mitigate further harm;

C. For equitable relief compelling Blackbaud to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Blackbaud's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

#### **X. JURY TRIAL DEMAND**

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 9th day of April, 2021

Respectfully submitted,

/s/ Marlon E. Kimpson

Marlon E. Kimpson (SC Bar No. 17042)

**MOTLEY RICE LLC**

28 Bridgeside Boulevard

Mount Pleasant, SC 29464

Tel.: (843) 216-9000

Fax: (843) 216-9027

Email: mkimpson@motleyrice.com

Amy E. Keller

**DICELLO LEVITT GUTZLER LLC**

Ten North Dearborn Street, Sixth Floor  
Chicago, IL 60602  
Tel: (312) 214-7900  
Fax: (312) 253-1443  
Email: akeller@dicellolevitt.com

Krysta Kauble Pachman  
**SUSMAN GODFREY LLP**  
1900 Avenue of the Stars, Suite 1400  
Los Angeles, CA 90067  
Tel: (310) 789-3100  
Fax: (310) 789-3150  
Email: kpachman@susmangodfrey.com

Harper Segui  
**WHITFIELD BRYSON LLP**  
Federal ID No. 10841  
217 Lucas Street, Suite G  
Mount Pleasant, SC 29464  
Tel: (919) 600-5000  
Fax: (919) 600-5035  
Email: harper@whitfieldbryson.com

***Plaintiffs' Co-Lead Counsel in the Pending Consumer MDL***

Gretchen Freeman Cappio  
**KELLER ROHRBACK L.L.P.**  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
Email: gcappio@kellerrohrback.com

***Chair of Plaintiffs' Steering Committee in the Pending Consumer MDL***

Desiree Cummings  
**ROBBINS GELLER RUDMAN & DOWD LLP**  
420 Lexington Avenue, Suite 1832  
New York, NY 10170  
Tel: (212) 693-1058  
Email: dcummings@rgrdlaw.com

Melissa Emert

**KANTROWITZ, GOLDHAMMER &  
GRAIFMAN, PC**

747 Chestnut Ridge Road  
Chestnut Ridge, NY 10977  
Tel: (866) 574-4682  
Fax: (845) 356-4335  
Email: [memert@kgglaw.com](mailto:memert@kgglaw.com)

Kelly Iverson

**CARLSON LYNCH**

1133 Penn Avenue, 5th Floor  
Pittsburgh, PA 15222  
Tel: (412) 322-9243  
Fax: (412) 231-0246  
Email: [kiverson@carlsonlynch.com](mailto:kiverson@carlsonlynch.com)

Howard Longman

**STULL, STULL & BRODY**

6 E 45th Street  
New York, NY 10017  
Tel: (973) 994-2315  
Fax: (973) 994-2319  
Email: [hlongman@ssbny.com](mailto:hlongman@ssbny.com)

Douglas McNamara

**COHEN MILSTEIN SELLERS  
& TOLL PLLC**

1100 New York Avenue NW  
East Tower, 5th Floor  
Washington, DC 20005  
Tel: (202) 408-4600  
Fax: (202) 408-4699  
Email: [dmcnamara@cohenmilstein.com](mailto:dmcnamara@cohenmilstein.com)

Melissa Weiner

**PEARSON, SIMON & WARSHAW, LLP**

800 LaSalle Avenue, Suite 2150  
Minneapolis, MN 55402  
Tel: (612) 389-0600  
Fax: (612) 389-0610  
Email: [mweiner@pswlaw.com](mailto:mweiner@pswlaw.com)

***Plaintiffs' Steering Committee in the Pending Consumer  
MDL***

Frank Ulmer  
**MCCULLEY MCCLUER LLC**  
701 East Bay Street, Suite 411  
Charleston, SC 29403  
Tel: (843) 444-5404  
Fax: (843) 444-5408  
Email: fulmer@mcculleymccluer.com

*Plaintiffs' Liaison Counsel*